XIX.

Über die Diskriminanten endlicher Körper.

[Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen. Bd. 29, S. 1—56 (1882).]

Unter den charakteristischen Zahlen oder Invarianten, von denen die Eigenschaften eines endlichen Zahlkörpers Ω abhängen, ist nächst dem Grade vor allem die Grundzahl oder Diskriminante $\Delta(\Omega)$ zu nennen*), und es ist von großer Wichtigkeit für die Zahlentheorie und Algebra, die Bildung dieser ganzen rationalen Zahl auf allgemeine Gesetze zurückzuführen. In den Göttingischen gelehrten Anzeigen vom 20. September 1871 (S. 1490) habe ich zuerst einen hierauf bezüglichen Satz ohne Beweis mitgeteilt, durch welchen die in der Grundzahl aufgehenden Primzahlen bestimmt werden; so einfach und naheliegend dieser Satz ist, so war es mir doch erst nach vielen vergeblichen Anstrengungen im Juli 1871 gelungen, ihn streng und allgemein zu beweisen; es treten nämlich hierbei dieselben eigentümlichen Umstände als hemmende Schwierigkeiten auf, die ich schon damals erwähnt habe, und die später in der Abhandlung**) Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen eingehend dargestellt sind. In der gegenwärtigen Abhandlung, welche als eine Fortsetzung der eben genannten anzusehen ist, werden zunächst zwei verschiedene Beweise für den oben erwähnten Satz gegeben, in § 3 ein unvollständiger, in den §§ 4—6 ein vollständiger, welcher im wesentlichen mit dem im Juli 1871 gefundenen übereinstimmt. Der übrige, und zwar größere Teil der Abhandlung ist aber einer genaueren Untersuchung der Grundzahl gewidmet und führt zu einem allgemeinen Gesetze, von welchem die Konstitution dieser Zahl beherrscht wird; das Resultat, zu welchem man gelangt, besteht darin, daß die Grund-

*) Hinsichtlich der von mir benutzten Kunstausdrücke muß ich auf meine anderen Schriften verweisen, namentlich auf das Supplement XI in der dritten Auflage der Vorlesungen über Zahlentheorie von Dirichlet, die ich im folgenden mit Z. zitieren werde.

**) Bd. 23 dieser Abhandlungen, 1878. Dieselbe soll mit G. zitiert werden.

www.rcin.org.pl

zahl, absolut genommen, immer die Norm eines Ideals ist, welches ich das Grundideal des Körpers Ω nenne, und dessen Zusammensetzung aus Primidealen, abgesehen von gewissen singulären Fällen, vollständig bestimmt wird; und hieraus folgt ohne weiteres ein dritter Beweis des oben erwähnten Satzes.

Dieser Satz gestattet, was ich schon am Schlusse der früheren Abhandlung ausgesprochen habe, noch eine wesentliche Erweiterung, und ich füge hinzu, daß dasselbe auch von allen übrigen in der vorliegenden Abhandlung gewonnenen Resultaten gilt. Zu dieser wichtigen Verallgemeinerung gelangt man, wenn man den Körper der rationalen Zahlen, soweit er als solcher in unserer Untersuchung auftritt, überall durch einen beliebigen in Ω als Divisor enthaltenen Körper ersetzt; die Modifikationen, welche unsere Resultate hierdurch erleiden, bestehen im wesentlichen nur darin, daß neben den gewöhnlichen Normen, Diskriminanten, Spuren auch partielle oder relative, auf diesen Körper bezügliche Normen usw. einzuführen, und gewisse rationale Zahlen durch Ideale dieses Körpers zu ersetzen sind. Da aber diese Erweiterung mancherlei Vorbereitungen und einen beträchtlichen Raum erfordert, so muß ihre Darstellung einer besonderen Abhandlung vorbehalten bleiben.

§ 1.

Ist Ω ein endlicher Körper n^{ten} Grades (Z. §§ 162—164), so geht derselbe durch n Permutationen $\varphi^{(1)}, \varphi^{(2)} \dots \varphi^{(n)}$ in n konjugierte Körper $\Omega^{(1)}, \Omega^{(2)} \dots \Omega^{(n)}$ über, und wir wollen, wenn θ irgend eine Zahl in Ω bedeutet, mit $\theta^{(1)}, \theta^{(2)} \dots \theta^{(n)}$ die konjugierten Zahlen bezeichnen, welche durch diese Permutationen aus θ erzeugt werden. Führt man eine Variable t ein, so entspricht jeder Zahl θ eine zugehörige ganze Funktion

$$(1) \qquad \begin{aligned} F(t) &= (t-\theta^{(1)})(t-\theta^{(2)})\dots(t-\theta^{(n)}) \\ &= t^n + a_1 t^{n-1} + a_2 t^{n-2} + \dots + a_{n-1} t + a_n, \end{aligned}$$

deren Koeffizienten rationale Zahlen $1, a_1, a_2 \dots a_n$ sind. Diese Funktion erhält man auch auf folgende Weise. Bilden die n Zahlen $\omega_1, \omega_2 \dots \omega_n$ eine beliebige Basis des Körpers Ω, so kann man

$$(2) \qquad \begin{aligned} \theta\omega_1 &= e_{1,1}\omega_1 + e_{2,1}\omega_2 + \dots + e_{n,1}\omega_n \\ \theta\omega_2 &= e_{1,2}\omega_1 + e_{2,2}\omega_2 + \dots + e_{n,2}\omega_n \\ &\dots\dots\dots\dots\dots\dots \\ \theta\omega_n &= e_{1,n}\omega_1 + e_{2,n}\omega_2 + \dots + e_{n,n}\omega_n \end{aligned}$$

www.rcin.org.pl

setzen, wo die Koeffizienten $e_{r,s}$ rationale Zahlen bedeuten, und es ist

$$(3)\qquad (-1)^n F(t) = \begin{vmatrix} e_{1,1}-t, & e_{2,1} & \dots e_{n,1} \\ e_{1,2}, & e_{2,2}-t & \dots e_{n,2} \\ \dots & \dots & \dots \\ e_{1,n}, & e_{2,n} & \dots e_{n,n}-t \end{vmatrix}.$$

Die mit $N(\theta)$ zu bezeichnende Norm der Zahl θ ist das Produkt aus allen mit θ konjugierten Zahlen, also

$$(4)\qquad N(\theta) = \theta^{(1)}\theta^{(2)}\dots\theta^{(n)} = (-1)^n a_n = \begin{vmatrix} e_{1,1}\dots e_{n,1} \\ \dots \\ e_{1,n}\dots e_{n,n} \end{vmatrix}.$$

Die der Zahl θ entsprechende Funktion $F(t)$ kann daher auch dadurch definiert werden, daß für jeden rationalen Wert von t

$$(5)\qquad F(t) = N(t-\theta)$$

ist.

Da die Funktion $F(t)$, also auch ihre Derivierte $F'(t)$ durch die Zahl θ vollständig bestimmt ist, so gilt dasselbe von der Zahl $F'(\theta)$, welche wir zur Abkürzung mit θ^* bezeichnen wollen, weil sie häufig auftreten wird; bedeutet $\varphi^{(1)}$ die identische Permutation des Körpers Ω (d. h. diejenige, durch welche jede Zahl θ in sich selbst übergeht), so ist hiernach

$$(6)\qquad \begin{aligned} \theta^* = F'(\theta) &= (\theta-\theta^{(2)})(\theta-\theta^{(3)})\dots(\theta-\theta^{(n)}) \\ &= n\,\theta^{n-1} + (n-1)\,a_1\,\theta^{n-2} + \dots + a_{n-1}; \end{aligned}$$

bekanntlich ist die Funktion $F(t)$ stets und nur dann irreduktibel, wenn diese Zahl θ^* nicht verschwindet.

Die Diskriminante $\Delta(\alpha_1, \alpha_2 \dots \alpha_n)$ eines beliebigen Systems von n Zahlen $\alpha_1, \alpha_2 \dots \alpha_n$, welche dem Körper Ω angehören, ist das Quadrat der aus den konjugierten Zahlen $\alpha_r^{(s)}$ gebildeten Determinante, also

$$(7)\qquad \Delta(\alpha_1, \alpha_2 \dots \alpha_n) = \begin{vmatrix} \alpha_1^{(1)}, & \alpha_2^{(1)} \dots \alpha_n^{(1)} \\ \alpha_1^{(2)}, & \alpha_2^{(2)} \dots \alpha_n^{(2)} \\ \dots & \dots \\ \alpha_1^{(n)}, & \alpha_2^{(n)} \dots \alpha_n^{(n)} \end{vmatrix}^2;$$

sie ist stets und nur dann von Null verschieden, wenn $\alpha_1, \alpha_2 \dots \alpha_n$ eine Basis des Körpers Ω bilden. Ist

$$(8)\qquad \begin{cases} \alpha_1 = a_{1,1}\omega_1 + a_{2,1}\omega_2 + \dots + a_{n,1}\omega_n \\ \alpha_2 = a_{1,2}\omega_1 + a_{2,2}\omega_2 + \dots + a_{n,2}\omega_n \\ \dots \\ \alpha_n = a_{1,n}\omega_1 + a_{2,n}\omega_2 + \dots + a_{n,n}\omega_n, \end{cases}$$

www.rcin.org.pl

wo die Koeffizienten $a_{r,s}$ rationale Zahlen bedeuten, so ist

$$(9) \qquad \Delta(\alpha_1, \alpha_2 \dots \alpha_n) = (\sum \pm a_{1,1} a_{2,2} \dots a_{n,n})^2 \Delta(\omega_1, \omega_2 \dots \omega_n).$$

Die oben definierten Zahlen θ^* stehen in naher Beziehung zum Begriff der Diskriminante, denn es ist bekanntlich

$$(10) \qquad \Delta(1, \theta, \theta^2 \dots \theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N(\theta^*).$$

Unter der Spur der Zahl θ verstehen wir die Summe aller mit ihr konjugierten Zahlen; wir bezeichnen diese offenbar rationale Zahl mit $S(\theta)$; dann ist

$$(11) \qquad \begin{aligned} S(\theta) &= \theta^{(1)} + \theta^{(2)} + \dots + \theta^{(n)} = -a_1 \\ &= e_{1,1} + e_{2,2} + \dots + e_{n,n}, \end{aligned}$$

wo a_1 und die Größen $e_{r,s}$ dieselbe Bedeutung haben, wie in (1) und (2). Über den Gebrauch dieses Zeichens ist folgendes zu merken. Da jede rationale Zahl durch alle Permutationen in sich selbst übergeht, so ist

$$(12) \qquad S(0) = 0, \quad S(1) = n;$$

da ferner $(\alpha \pm \beta)^{(r)} = \alpha^{(r)} \pm \beta^{(r)}$, und $(\alpha\beta)^{(r)} = \alpha^{(r)}\beta^{(r)}$ ist, so folgt

$$(13) \qquad S(\alpha \pm \beta) = S(\alpha) \pm S(\beta),$$

und wenn c rational ist,

$$(14) \qquad S(c\alpha) = c\,S(\alpha).$$

Ferner folgt aus

$$S(\alpha\beta) = \alpha^{(1)}\beta^{(1)} + \alpha^{(2)}\beta^{(2)} + \dots + \alpha^{(n)}\beta^{(n)}$$

nach dem Satze über die Multiplikation der Determinanten

$$(15) \qquad \sum \pm \alpha_1^{(1)} \alpha_2^{(2)} \dots \alpha_n^{(n)} \cdot \sum \pm \beta_1^{(1)} \beta_2^{(2)} \dots \beta_n^{(n)} = \begin{vmatrix} S(\alpha_1\beta_1) \dots S(\alpha_1\beta_n) \\ \dots\dots\dots\dots \\ S(\alpha_n\beta_1) \dots S(\alpha_n\beta_n) \end{vmatrix},$$

mithin

$$(16) \qquad \Delta(\alpha_1, \alpha_2 \dots \alpha_n) = \begin{vmatrix} S(\alpha_1\alpha_1), S(\alpha_1\alpha_2) \dots S(\alpha_1\alpha_n) \\ S(\alpha_2\alpha_1), S(\alpha_2\alpha_2) \dots S(\alpha_2\alpha_n) \\ \dots\dots\dots\dots\dots\dots \\ S(\alpha_n\alpha_1), S(\alpha_n\alpha_2) \dots S(\alpha_n\alpha_n) \end{vmatrix}.$$

Hat eine Zahl α die Eigenschaft, daß für jede in $\mathfrak{Q}$ enthaltene Zahl ω die Spur $S(\alpha\omega)$ verschwindet, so ist gewiß $\alpha = 0$, weil

www.rcin.org.pl

sonst für $\omega = \alpha^{-1}$ sich ein Widerspruch mit (12) ergeben würde; und hieraus folgt mit Rücksicht auf (13) allgemeiner, daß, wenn für jede Zahl ω die Gleichung

(17) $$S(\alpha\omega) = S(\beta\omega)$$

gilt, notwendig

(18) $$\alpha = \beta$$

ist.

§ 2.

Der Inbegriff $\mathfrak{o}$ aller in Ω enthaltenen ganzen Zahlen (Z. § 166) ist ein endlicher Modul

(1) $$\mathfrak{o} = [\omega_1, \omega_2 \dots \omega_n],$$

d. h. es gibt n ganze Zahlen $\omega_1, \omega_2 \dots \omega_n$ von der Beschaffenheit, daß jede ganze Zahl ω in der Form

(2) $$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n$$

darstellbar ist, wo die Koeffizienten $h_1, h_2 \cdots h_n$ ganze rationale Zahlen bedeuten. Dieses System heißt eine Basis von $\mathfrak{o}$, und seine Diskriminante

(3) $$D = \Delta(\omega_1, \omega_2 \cdots \omega_n),$$

welche eine von Null verschiedene ganze rationale Zahl ist, heißt die Grundzahl oder Diskriminante des Körpers Ω.

Sind $\alpha_1, \alpha_2 \cdots \alpha_n$ ganze Zahlen, so sind die in den Gleichungen (8) und (9) des vorigen Paragraphen auftretenden rationalen Koeffizienten $a_{r,s}$ ganze Zahlen; folglich ist die Diskriminante $\Delta(\alpha_1, \alpha_2 \cdots \alpha_n)$ teilbar durch D (und nur dann $= D$, wenn diese Zahlen ebenfalls eine Basis von $\mathfrak{o}$ bilden). Ist θ eine ganze Zahl, so kann man dies auf das System $1, \theta, \theta^2 \cdots \theta^{n-1}$ anwenden und erhält

(4) $$\Delta(1, \theta, \theta^2 \cdots \theta^{n-1}) = Dk^2 = \pm N(\theta^*),$$

wo k eine ganze rationale Zahl ist, die wir, wie früher (G. § 1), den Index der Zahl θ nennen wollen.

Ist ω eine beliebige ganze Zahl, so gilt dasselbe von den mit ihr konjugierten Zahlen, mithin ist die Spur $S(\omega)$ eine ganze rationale Zahl; und wenn ω durch die ganze rationale Zahl c teilbar ist, so ist $S(\omega)$ ebenfalls durch c teilbar, weil $\omega = c\alpha$, also $S(\omega) = cS(\alpha)$, und $S(\alpha)$ ganz ist.

www.rcin.org.pl

Mit p bezeichnen wir im folgenden immer eine (positive) rationale Primzahl; dann folgt aus einer bekannten Eigenschaft der zum Exponenten p gehörenden Binomial-Koeffizienten, daß, wenn μ, ν irgend zwei ganze algebraische Zahlen bedeuten, immer

$$(\mu + \nu)^p = \mu^p + \nu^p + p\varrho \tag{5}$$

ist, wo ϱ ebenfalls eine ganze Zahl ist. Hieraus folgt, wenn ω irgend eine Zahl in $\mathfrak{o}$ bedeutet, zunächst

$$S(\omega)^p = (\omega^{(1)} + \omega^{(2)} + \cdots + \omega^{(n)})^p \equiv S(\omega^p) \pmod{p};$$

da aber $S(\omega)$ eine ganze rationale Zahl, mithin nach dem Satze von Fermat

$$S(\omega)^p \equiv S(\omega) \pmod{p}$$

ist, so ergibt sich

$$S(\omega) \equiv S(\omega^p) \pmod{p}, \tag{6}$$

und allgemeiner, wenn man ω immer durch ω^p ersetzt,

$$S(\omega) \equiv S(\omega^{p^m}) \pmod{p}. \tag{7}$$

Sind $\alpha_1, \alpha_2 \cdots \alpha_n$ beliebige Zahlen in $\mathfrak{o}$, so folgt hieraus mit Rücksicht auf die Gleichung (16) des vorigen Paragraphen der Satz

$$\Delta(\alpha_1^p, \alpha_2^p \cdots \alpha_n^p) \equiv \Delta(\alpha_1, \alpha_2 \cdots \alpha_n) \pmod{p}. \tag{8}$$

Ebenso ergibt sich aus (7) unmittelbar der folgende (nicht umzukehrende) Satz: Wenn ω durch alle in p aufgehenden Primideale teilbar ist, so ist

$$S(\omega) \equiv 0 \pmod{p}; \tag{9}$$

denn wenn man den Exponenten m hinreichend groß wählt, so wird die Zahl ω^{p^m} durch p teilbar.

§ 3.

Wir wenden uns nun zum Beweise des in der Einleitung erwähnten Satzes:

Die rationale Primzahl p geht stets und nur dann in der Grundzahl D des Körpers Ω auf, wenn p in diesem Körper durch das Quadrat eines Primideals teilbar ist.

Am Schlusse der früheren Abhandlung (G. § 5) ist bemerkt, daß dieser Beweis, falls es in $\mathfrak{o}$ eine Zahl θ gibt, deren Index k nicht teilbar durch p ist, leicht aus den dort gewonnenen Resultaten abgeleitet werden kann. Dies soll zunächst geschehen.

www.rcin.org.pl

In der Tat, wenn es eine solche Zahl θ gibt, so ist damals gezeigt (G. § 2), daß die Zerlegung des Ideals $\mathfrak{o}p$ in Primfaktoren auf die Zerlegung der zugehörigen Funktion $F(t)$ in Primfunktionen nach dem Modul p zurückkommt. Ist nämlich

$$F(t) \equiv P(t)^e P_1(t)^{e_1} \cdots \pmod{p},$$

wo $P(t)$, $P_1(t) \cdots$ wesentlich verschiedene Primfunktionen bedeuten, so entsprechen denselben ebenso viele verschiedene Primideale $\mathfrak{p}, \mathfrak{p}_1 \cdots$, und gleichzeitig gilt die Zerlegung

$$\mathfrak{o}p = \mathfrak{p}^e \mathfrak{p}_1^{e_1} \cdots;$$

ist ferner $\psi(t)$ eine beliebige ganze Funktion von t mit ganzen rationalen Koeffizienten, so ist die ganze Zahl $\psi(\theta)$ stets und nur dann durch das Primideal $\mathfrak{p}$ teilbar, wenn $\psi(t)$ nach dem Modul p durch die entsprechende Primfunktion $P(t)$ teilbar ist. Verbinden wir hiermit den allgemeinen Satz*), daß eine Funktion $F(t)$ und ihre Derivierte $F'(t)$ stets und nur dann durch eine und dieselbe Primfunktion $P(t)$ nach p teilbar sind, wenn $F(t)$ durch das Quadrat von $P(t)$ teilbar ist, so ergibt sich folgendes.

Wenn p durch das Quadrat eines Primideals teilbar ist, so muß einer der Exponenten $e, e_1 \cdots$, z. B. $e > 1$ sein; dann ist $F'(t)$ durch $P(t)$, folglich die Zahl θ^* durch $\mathfrak{p}$ teilbar; mithin geht die Norm von $\mathfrak{p}$, welche immer durch p teilbar, nämlich eine Potenz von p ist, in der Norm von θ^* auf (Z. § 169, 5.); hieraus folgt mit Rücksicht auf die Gleichung (4) in § 2, daß Dk^2 durch p teilbar ist, und da p nicht in k aufgeht, so muß die Grundzahl D durch p teilbar sein.

Wenn aber p durch kein Primideal-Quadrat teilbar ist, so sind die Exponenten $e, e_1 \cdots$ sämtlich $= 1$; dann ist $F'(t)$ durch keine der Primfunktionen $P(t), P_1(t) \cdots$ teilbar, und folglich ist die Zahl θ^* auch durch keines der Primideale $\mathfrak{p}, \mathfrak{p}_1 \cdots$ teilbar; mithin ist θ^* relative

*) In meiner Abhandlung über die Theorie der höheren Kongruenzen (Borchardts Journal, Bd. 54, S. 7), die ich im folgenden wieder mit K. zitieren werde, ist zwar nur der erste Teil bewiesen, daß $F'(t)$ gewiß durch $P(t)$ teilbar ist, wenn $P(t)^2$ in $F(t)$ aufgeht; bedenkt man aber, daß die Derivierte $P'(t)$ niemals $\equiv 0 \pmod{p}$ ist (weil sonst die Primfunktion $P(t)$ der p^{ten} Potenz einer Funktion kongruent wäre), und daß folglich $P'(t)$ auch nicht durch $P(t)$ teilbar sein kann (weil der Grad von $P'(t)$ kleiner als der von $P(t)$ ist), so ergibt sich auch der andere Teil des obigen Satzes.

www.rcin.org.pl

Primzahl zu p, und hieraus folgt (Z. § 174, 8), daß ihre Norm $\pm D k^2$, und also auch deren Teiler D nicht durch p teilbar ist.

Hiermit ist der obige Satz vollständig bewiesen, aber nur unter der Voraussetzung der Existenz einer Zahl θ, deren Index k nicht durch p teilbar ist; da nun in der früheren Abhandlung (G. § 5) gezeigt ist, daß es Körper Ω gibt, bei denen diese Voraussetzung nicht für alle Primzahlen p zutrifft, so bedarf es eines anderen Beweises, um die Wahrheit des Satzes für alle Fälle außer Zweifel zu setzen.

§ 4.

Der zu beweisende Satz zerfällt in zwei Teile, von denen der eine in folgender Form ausgesprochen werden kann:

Ist p durch das Quadrat eines Primideals teilbar, so geht p in der Grundzahl D auf.

Dies ist sehr leicht zu beweisen. Denn wenn $\mathfrak{o}\,p = \mathfrak{a}\,\mathfrak{p}^2$ ist, wo $\mathfrak{p}$ ein Primideal (oder auch irgend ein von $\mathfrak{o}$ verschiedenes Ideal) bedeutet, so ist $\mathfrak{a}\,\mathfrak{p}$ nicht teilbar durch $\mathfrak{o}\,p$, und es gibt folglich in $\mathfrak{a}\,\mathfrak{p}$ eine durch p nicht teilbare Zahl ω; da ferner $(\mathfrak{a}\,\mathfrak{p})^2 = \mathfrak{a}\,p$, also durch $\mathfrak{o}\,p$ teilbar ist, so geht p in ω^2, also auch in ω^p auf. Setzt man nun wieder

$$\mathfrak{o} = [\omega_1, \omega_2 \cdots \omega_n],$$

also

$$D = \Delta(\omega_1, \omega_2 \cdots \omega_n),$$

so ist

$$\omega = \sum h_\iota \omega_\iota,$$

wo die ganzen rationalen Koordinaten $h_1, h_2 \cdots h_n$ nicht alle durch p teilbar sind, weil sonst auch ω durch p teilbar wäre, was nicht der Fall ist. Erhebt man zur p^{ten} Potenz, so folgt aus dem Satze (5) in § 2 mit Rücksicht auf den Satz von Fermat

$$\omega^p \equiv \sum (h_\iota \omega_\iota)^p \equiv \sum h_\iota \omega_\iota^p \pmod{p},$$

und da ω^p durch p teilbar ist, so ist auch

$$\sum h_\iota \omega_\iota^p \equiv 0 \pmod{p}.$$

Da aber die Zahlen h_ι, wie oben bemerkt, nicht alle durch p teilbar sind, so folgt aus einem früher bewiesenen Satze (Z. § 166, (1)), daß die Diskriminante

$$\Delta(\omega_1^p, \omega_2^p \cdots \omega_n^p)$$

www.rcin.org.pl

durch p (sogar durch p^2) teilbar ist*), und hieraus ergibt sich nach dem Satze (8) in § 2, daß p auch in D aufgeht, w. z. b. w.

§ 5.

Bei weitem schwieriger ist der zweite Teil des Satzes, die Umkehrung des ersten Teils, zu beweisen, und wir müssen zunächst einige Hilfssätze entwickeln, die aber auch für verwandte Untersuchungen von Nutzen sind.

1. Satz: Ist die aus lauter ganzen rationalen Zahlen $c_{r,s}$ gebildete Determinante n^{ten} Grades

$$C = \begin{vmatrix} c_{1,1}, & c_{2,1} \cdots c_{n,1} \\ c_{1,2}, & c_{2,2} \cdots c_{n,2} \\ \cdots & \cdots \\ c_{1,n}, & c_{2,n} \cdots c_{n,n} \end{vmatrix}$$

teilbar durch die Primzahl p, so kann man n ganze rationale Zahlen $x_1, x_2 \cdots x_n$, die nicht alle durch p teilbar sind, so wählen, daß die n Kongruenzen

$$\left.\begin{aligned} c_{1,1}x_1 + c_{1,2}x_2 + \cdots + c_{1,n}x_n &\equiv 0 \\ c_{2,1}x_1 + c_{2,2}x_2 + \cdots + c_{2,n}x_n &\equiv 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ c_{n,1}x_1 + c_{n,2}x_2 + \cdots + c_{n,n}x_n &\equiv 0 \end{aligned}\right\} \pmod{p}$$

erfüllt werden**).

Dies leuchtet von selbst ein, wenn alle Koeffizienten $c_{r,s}$ durch p teilbar sind. Im entgegengesetzten Falle wird es eine Unterdeterminante C' von höchstem Grade $m < n$ geben, welche nicht durch p teilbar ist, und wir dürfen annehmen, es sei

$$C' = \begin{vmatrix} c_{1,1}, & c_{1,2} \cdots c_{1,m} \\ c_{2,1}, & c_{2,2} \cdots c_{2,m} \\ \cdots & \cdots \\ c_{m,1}, & c_{m,2} \cdots c_{m,m} \end{vmatrix};$$

dann genügt man allen vorstehenden Kongruenzen z. B. dadurch,

*) Dies gilt offenbar auch dann, wenn die Potenzen $\omega_1^p, \omega_2^p \cdots \omega_n^p$ keine Basis des Körpers Ω bilden, weil in diesem Falle ihre Diskriminante verschwindet, also durch p teilbar ist.

**) Von demselben Satze ist auch schon in der früheren Abhandlung (G. § 1) Gebrauch gemacht; der Vollständigkeit wegen soll jetzt der Beweis nachgeholt werden.

www.rcin.org.pl

daß man

$$x_{m+2} = 0, \quad x_{m+3} = 0 \cdots x_n = 0$$

und für $x_1, x_2 \cdots x_m, x_{m+1}$ resp. die Koeffizienten setzt, mit welchen die unbestimmten Größen $u_1, u_2 \cdots u_m, u_{m+1}$ in der Determinante

$$\begin{vmatrix} c_{1,1}, & c_{1,2} \cdots c_{1,m}, & c_{1,m+1} \\ c_{2,1}, & c_{2,2} \cdots c_{2,m}, & c_{2,m+1} \\ \cdots\cdots & \cdots\cdots\cdots & \cdots\cdots \\ c_{m,1}, & c_{m,2} \cdots c_{m,m}, & c_{m,m+1} \\ u_1, & u_2 \quad \cdots u_m, & u_{m+1} \end{vmatrix}$$

multipliziert sind; denn diese Determinante

$$u_1 x_1 + u_2 x_2 + \cdots + u_m x_m + u_{m+1} x_{m+1}$$

wird zufolge unserer Annahme immer eine durch p teilbare Zahl, sobald

$$u_1 = c_{r,1}, \quad u_2 = c_{r,2} \cdots u_m = c_{r,m}, \quad u_{m+1} = c_{r,m+1}$$

gesetzt wird. Und da $x_{m+1} = C'$, also nicht durch p teilbar ist, so ist der Satz bewiesen*).

2. Sind $\alpha_1, \alpha_2 \cdots \alpha_r$ bestimmte Zahlen in $\mathfrak{o}$, während $x_1, x_2 \cdots x_r$ willkürliche ganze rationale Zahlen bedeuten, so bilden die Zahlen

$$\alpha = x_1 \alpha_1 + x_2 \alpha_2 + \cdots + x_r \alpha_r$$

einen durch $\mathfrak{o}$ teilbaren endlichen Modul $\mathfrak{a} = [\alpha_1, \alpha_2 \cdots \alpha_r]$, und die Anzahl $(\mathfrak{a}, \mathfrak{o}\, p)$ der in $\mathfrak{a}$ enthaltenen, nach p inkongruenten Zahlen ist offenbar höchstens $= p^r$; sie wird stets und nur dann genau $= p^r$ sein, wenn die Zahlen $\alpha_1, \alpha_2 \cdots \alpha_r$ die Eigenschaft haben, daß die Kongruenz $\alpha \equiv 0 \pmod{p}$ nur durch $x_1 \equiv 0, x_2 \equiv 0 \cdots x_r \equiv 0 \pmod{p}$ befriedigt werden kann; in diesem Fall wollen wir sagen, daß die Zahlen $\alpha_1, \alpha_2 \cdots \alpha_r$ ein nach p irreduktibeles System bilden, und es leuchtet ein, daß $r \leqq n$ ist, weil $(\mathfrak{o}, \mathfrak{o}\, p) = p^n$ ist. Bilden die Zahlen $\alpha_1, \alpha_2 \cdots \alpha_r$ aber ein nach p reduktibeles System, gibt es also ganze rationale Zahlen $a_1, a_2 \cdots a_r$, welche die Kongruenz

$$a_1 \alpha_1 + a_2 \alpha_2 + \cdots + a_r \alpha_r \equiv 0 \pmod{p}$$

befriedigen, und von denen wenigstens eine, z. B. a_r, nicht durch p teilbar ist, so kann man, weil p eine Primzahl ist, eine ganze rationale Zahl a' so bestimmen, daß $a' a_r \equiv 1 \pmod{p}$ wird; multipliziert

*) Ersetzt man die oben benutzten Elemente $c_{r,m+1}$ sukzessive durch $c_{r,m+2}$, $c_{r,m+3} \cdots c_{r,n}$, so erhält man im ganzen $n - m$ partikuläre Lösungen der gegebenen Kongruenzen, aus welchen ihre allgemeinste Lösung leicht abzuleiten ist.

www.rcin.org.pl

man die obige Kongruenz mit α', so folgt, daß

$$\alpha_r \equiv b_1\alpha_1 + b_2\alpha_2 + \cdots + b_{r-1}\alpha_{r-1} \pmod{p}$$

ist, wo $b_1, b_2 \cdots b_{r-1}$ ganze rationale Zahlen bedeuten, und hieraus ergibt sich, daß jede Zahl α des Moduls $\mathfrak{a}$ mit einer Zahl α' des Moduls $\mathfrak{a}' = [\alpha_1, \alpha_2 \cdots \alpha_{r-1}]$ nach p kongruent ist; da ferner $\mathfrak{a}'$ teilbar durch $\mathfrak{a}$, d. h. da jede Zahl α' auch in $\mathfrak{a}$ enthalten ist, so folgt $(\mathfrak{a}, \mathfrak{o}\,p) = (\mathfrak{a}', \mathfrak{o}\,p)$, und diese Anzahl ist höchstens $= p^{r-1}$. Ist das System $\alpha_1, \alpha_2 \cdots \alpha_{r-1}$ ebenfalls reduktibel nach p, so kann man in derselben Weise fortfahren, bis man zu einem nach p irreduktibelen System gelangt; besteht dasselbe aus m Zahlen, so ist

$$(\mathfrak{a}, \mathfrak{o}\,p) = p^m;$$

die Zahl m ist dadurch charakterisiert, daß es m Zahlen $\alpha'_1, \alpha'_2 \cdots \alpha'_m$ in $\mathfrak{a}$ gibt, welche ein nach p irreduktibeles System bilden, während jedes aus $(m+1)$ Zahlen des Moduls $\mathfrak{a}$ gebildete System reduktibel nach p ist; ist α eine beliebige Zahl in $\mathfrak{a}$, so gibt es immer m ganze rationale Zahlen $y_1, y_2 \cdots y_m$, welche die Kongruenz

$$\alpha \equiv y_1\alpha'_1 + y_2\alpha'_2 + \cdots + y_m\alpha'_m \pmod{p}$$

befriedigen und in bezug auf den Modul p vollständig bestimmt sind. (Wenn $\mathfrak{a}$ durch $\mathfrak{o}\,p$ teilbar ist, so ist $m = 0$ zu setzen.)

3. Bilden die Zahlen $\omega_1, \omega_2 \cdots \omega_n$ eine Basis von $\mathfrak{o}$, und betrachtet man ein System von n ganzen Zahlen

$$\begin{aligned}
\alpha_1 &= c_{1,1}\omega_1 + c_{2,1}\omega_2 + \cdots + c_{n,1}\omega_n \\
\alpha_2 &= c_{1,2}\omega_1 + c_{2,2}\omega_2 + \cdots + c_{n,2}\omega_n \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
\alpha_n &= c_{1,n}\omega_1 + c_{2,n}\omega_2 + \cdots + c_{n,n}\omega_n,
\end{aligned}$$

so geht aus dem obigen Satze 1. hervor, daß dasselbe stets und nur dann nach p irreduktibel ist, wenn die aus den Koordinaten $c_{r,s}$ gebildete Determinante C nicht durch p teilbar ist. Unter dieser Voraussetzung gibt es daher, wenn ω eine gegebene ganze Zahl ist, immer n ganze rationale, nach dem Modul p vollständig bestimmte Zahlen $x_1, x_2 \cdots x_n$, welche die Kongruenz

$$\omega \equiv x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n \pmod{p}$$

befriedigen. Man kann daher auch

$$\left.\begin{aligned}
\omega\,\alpha_1 &\equiv x_{1,1}\alpha_1 + x_{2,1}\alpha_2 + \cdots + x_{n,1}\alpha_n \\
\omega\,\alpha_2 &\equiv x_{1,2}\alpha_1 + x_{2,2}\alpha_2 + \cdots + x_{n,2}\alpha_n \\
&\cdots\cdots\cdots\cdots\cdots\cdots \\
\omega\,\alpha_n &\equiv x_{1,n}\alpha_1 + x_{2,n}\alpha_2 + \cdots + x_{n,n}\alpha_n
\end{aligned}\right\} \pmod{p}$$

www.rcin.org.pl

setzen, wo die ganzen rationalen Zahlen $x_{r,s}$ nach dem Modul p bestimmt sind, und wir wollen den Satz*) beweisen, daß

$$S(\omega) \equiv x_{1,1} + x_{2,2} + \cdots + x_{n,n} \pmod{p}$$

ist.

In der Tat, da jede der Zahlen $\omega_1, \omega_2 \cdots \omega_n$ und folglich jede ganze Zahl durch Multiplikation mit C in eine Zahl des Moduls $[\alpha_1, \alpha_2 \cdots \alpha_n]$ verwandelt wird, so kann man

$$\begin{aligned} C\omega\alpha_1 &= y_{1,1}\alpha_1 + y_{2,1}\alpha_2 + \cdots + y_{n,1}\alpha_n \\ C\omega\alpha_2 &= y_{1,2}\alpha_1 + y_{2,2}\alpha_2 + \cdots + y_{n,2}\alpha_n \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ C\omega\alpha_n &= y_{1,n}\alpha_1 + y_{2,n}\alpha_2 + \cdots + y_{n,n}\alpha_n \end{aligned}$$

setzen, wo die Koeffizienten $y_{r,s}$ ganze rationale Zahlen bedeuten, welche offenbar mit den obigen Koeffizienten $x_{r,s}$ durch die Kongruenzen

$$y_{r,s} \equiv C x_{r,s} \pmod{p}$$

zusammenhängen; da andererseits (zufolge § 1, (11) und (14))

$$S(C\omega) = C S(\omega) = y_{1,1} + y_{2,2} + \cdots + y_{n,n},$$

und C nicht durch p teilbar ist, so ergibt sich die Richtigkeit der zu beweisenden Kongruenz.

4. Wir zerlegen nun das Ideal $\mathfrak{o}p$ auf irgend eine Weise in ein Produkt von zwei Idealen $\mathfrak{p}$, $\mathfrak{q}$, und bezeichnen deren Grade**) resp. mit r, s; dann ist

$$\mathfrak{o}p = \mathfrak{p}\mathfrak{q}; \quad N(\mathfrak{o}p) = p^n = N(\mathfrak{p})N(\mathfrak{q}) = p^r p^s,$$

also $r + s = n$. Da ferner (Z. § 173, 7)

$$(\mathfrak{q}, \mathfrak{o}p) = N(\mathfrak{p}) = p^r$$

ist, so gibt es (zufolge 2) in dem endlichen Modul $\mathfrak{q}$ ein System von r Zahlen

$$\varrho_0, \varrho_1 \cdots \varrho_{r-1},$$

welches irreduktibel nach p ist, und jede durch $\mathfrak{q}$ teilbare (d. h. in $\mathfrak{q}$ enthaltene) Zahl ist

$$\equiv h_0\varrho_0 + h_1\varrho_1 + \cdots + h_{r-1}\varrho_{r-1} \pmod{p},$$

---

*) Offenbar gelten ähnliche Sätze für $N(\omega)$ und alle übrigen Koeffizienten der zu ω zugehörigen Funktion n^{ten} Grades (§ 1).

**) Unter dem Grade eines beliebigen Ideals $\mathfrak{a}$ wird die Anzahl der (gleichen oder ungleichen) rationalen Primzahlen verstanden, deren Produkt $= N(\mathfrak{a})$ ist (vgl. Z. § 171, 10).

www.rcin.org.pl

wo h_0, $h_1 \cdots h_{r-1}$ ganze rationale Zahlen bedeuten. Ebenso gibt es in $\mathfrak{p}$ ein nach p irreduktibeles System von s Zahlen

$$\sigma_0, \sigma_1 \cdots \sigma_{s-1},$$

und jede durch $\mathfrak{p}$ teilbare Zahl ist

$$\equiv k_0\sigma_0 + k_1\sigma_1 + \cdots + k_{s-1}\sigma_{s-1} \pmod{p},$$

wo k_0, $k_1 \cdots k_{s-1}$ ebenfalls ganze rationale Zahlen bedeuten.

Wir nehmen nun ferner an, daß $\mathfrak{p}$, $\mathfrak{q}$ relative Primideale sind, daß also $\mathfrak{o}$ ihr größter gemeinschaftlicher Teiler ist; dann läßt sich leicht zeigen, daß die n Zahlen

$$\varrho_0, \varrho_1 \cdots \varrho_{r-1}, \quad \sigma_0, \sigma_1 \cdots \sigma_{s-1}$$

ebenfalls ein nach p irreduktibeles System bilden; da nämlich jede in $\mathfrak{o}$ enthaltene Zahl ω eine Summe von zwei Zahlen ist, deren eine in $\mathfrak{q}$, und deren andere in $\mathfrak{p}$ enthalten ist (Z. § 165 oder § 171), so ist auch

$$\omega \equiv h_0\varrho_0 + \cdots + h_{r-1}\varrho_{r-1} + k_0\sigma_0 + \cdots + k_{s-1}\sigma_{s-1} \pmod{p},$$

und hieraus ergibt sich unsere Behauptung (zufolge 2.), weil $(\mathfrak{o}, \mathfrak{o}\,p) = p^n = p^{r+s}$ ist. Dasselbe geht aber unmittelbar auch daraus hervor, daß die rechte Seite ω' der vorstehenden Kongruenz nur dann durch p teilbar wird, wenn alle n Koeffizienten h, $k \equiv 0 \pmod{p}$ sind; ist nämlich ω' durch p teilbar, so ist auch $\omega' \equiv 0 \pmod{\mathfrak{p}}$, mithin

$$h_0\varrho_0 + \cdots + h_{r-1}\varrho_{r-1} \equiv 0 \pmod{\mathfrak{p}},$$

weil die Zahlen σ_0, $\sigma_1 \cdots \sigma_{s-1}$ in $\mathfrak{p}$ enthalten sind; da nun die linke Seite dieser Kongruenz auch in $\mathfrak{q}$ enthalten ist, so ist sie, weil $\mathfrak{p}$, $\mathfrak{q}$ relative Primideale sind, auch durch $\mathfrak{p}\,\mathfrak{q}$, also durch p teilbar, und folglich müssen die r Koeffizienten h durch p teilbar sein, weil $\varrho_0, \varrho_1 \cdots \varrho_{r-1}$ ein nach p irreduktibeles System bilden; und auf dieselbe Weise ergibt sich, daß auch die s Koeffizienten k durch p teilbar sein müssen, was zu zeigen war.

Nachdem dieser Punkt festgestellt ist, wollen wir den in 3. bewiesenen Satz über die Spur $S(\omega)$ auf unser System ϱ_0, $\varrho_1 \cdots \varrho_{r-1}$, σ_0, $\sigma_1 \cdots \sigma_{s-1}$ und auf den Fall anwenden, daß ω eine beliebige durch $\mathfrak{q}$ teilbare Zahl μ ist. Da $\mathfrak{q}$ ein Ideal ist, so sind auch die r Produkte $\mu\varrho_0$, $\mu\varrho_1 \cdots \mu\varrho_{r-1}$ durch $\mathfrak{q}$ teilbar, und folglich wird

$$\left.\begin{aligned}
\mu\varrho_0 &\equiv h_{0,0}\varrho_0 + h_{1,0}\varrho_1 + \cdots + h_{r-1,0}\varrho_{r-1} \\
\mu\varrho_1 &\equiv h_{0,1}\varrho_0 + h_{1,1}\varrho_1 + \cdots + h_{r-1,1}\varrho_{r-1} \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\mu\varrho_{r-1} &\equiv h_{0,r-1}\varrho_0 + h_{1,r-1}\varrho_1 + \cdots + h_{r-1,r-1}\varrho_{r-1}
\end{aligned}\right\} \pmod{p}.$$

www.rcin.org.pl

Da ferner die übrigen s Produkte $\mu\sigma_0$, $\mu\sigma_1 \cdots \mu\sigma_{s-1}$ durch $\mathfrak{q}\mathfrak{p}$, also durch p teilbar sind, so werden in ihrer Darstellung durch die Zahlen ϱ, σ alle Koeffizienten h, $k \equiv 0 \pmod{p}$, und hieraus folgt nach dem in 3. bewiesenen Satze

$$S(\mu) \equiv h_{0,0} + h_{1,1} + \cdots + h_{r-1,r-1} \pmod{p}.$$

5. Wir nehmen jetzt, indem wir die bisherigen Voraussetzungen und Bezeichnungen beibehalten, ferner an, daß $\mathfrak{p}$ ein Primideal ist; unsere frühere Annahme, daß $\mathfrak{p}$ und $\mathfrak{q}$ relative Primideale sind, kommt also darauf hinaus, daß p nicht durch $\mathfrak{p}^2$ teilbar ist. Dann gilt der Satz, daß die Determinante

$$R = \begin{vmatrix} S(\varrho_0\varrho_0), & S(\varrho_0\varrho_1)\cdots & S(\varrho_0\varrho_{r-1}) \\ S(\varrho_1\varrho_0), & S(\varrho_1\varrho_1)\cdots & S(\varrho_1\varrho_{r-1}) \\ \cdots & \cdots & \cdots \\ S(\varrho_{r-1}\varrho_0), & S(\varrho_{r-1}\varrho_1)\cdots & S(\varrho_{r-1}\varrho_{r-1}) \end{vmatrix}$$

nicht durch p teilbar ist. Wir bemerken zunächst, daß dieser Satz, wenn er für ein bestimmtes System ϱ_0, $\varrho_1 \cdots \varrho_{r-1}$ bewiesen ist, auch für jedes andere System ϱ_0', $\varrho_1' \cdots \varrho_{r-1}'$ gelten muß, welches dem Ideal $\mathfrak{q}$ angehört und nach p irreduktibel ist; man kann nämlich

$$\left.\begin{array}{l} \varrho_0' \equiv a_{0,0}\,\varrho_0 + \cdots + a_{r-1,0}\,\varrho_{r-1} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \varrho_{r-1}' \equiv a_{0,r-1}\varrho_0 + \cdots + a_{r-1,r-1}\varrho_{r-1} \end{array}\right\} \pmod{p}$$

setzen, wo die aus den Koeffizienten $a_{\iota,\iota'}$ gebildete Determinante A nicht durch p teilbar ist, weil sonst (zufolge 1.) das System linker Hand reduktibel nach p wäre; da ferner, wenn die Summationsbuchstaben ι, ι' die Werte $0, 1 \cdots r-1$ durchlaufen,

$$\varrho_h'\varrho_k' \equiv \sum a_{\iota,h}\,a_{\iota',k}\,\varrho_\iota\varrho_{\iota'} \pmod{p},$$

also auch

$$S(\varrho_h'\varrho_k') \equiv \sum a_{\iota,h}\,a_{\iota',k}\,S(\varrho_\iota\varrho_{\iota'}) \pmod{p}$$

ist, so ergibt sich aus bekannten Determinanten-Sätzen, daß die aus den Spuren $S(\varrho_h'\varrho_k')$ gebildete Determinante $P_\iota' \equiv RA^2 \pmod{p}$ ist, woraus unsere obige Behauptung folgt.

Wir konstruieren nun ein bestimmtes nach p irreduktibeles System ϱ_0, $\varrho_1 \cdots \varrho_{r-1}$ auf folgende Weise. Da $\mathfrak{p}$ ein in p aufgehendes Primideal r^{ten} Grades ist, so wählen wir, wie in der früheren Abhandlung (G. § 4), eine ganze Funktion

$$(1) \qquad P(t) = t^r + a_1 t^{r-1} + \cdots + a_{r-1}t + a_r$$

www.rcin.org.pl

vom Grade r, welche ganze rationale Koeffizienten $1, a_1 \cdots a_{r-1}, a_r$ hat und eine Primfunktion in bezug auf den Modul p ist; dann hat die Kongruenz

(2) $$P(\alpha) \equiv 0 \pmod{\mathfrak{p}}$$

immer r inkongruente Wurzeln, und wir bezeichnen mit α eine bestimmte von ihnen (die übrigen sind dann $\alpha^p, \alpha^{p^2} \cdots \alpha^{p^{r-1}}$); sind ferner $x_0, x_1 \cdots x_{r-1}$ ganze rationale Zahlen, so kann, wie damals bewiesen ist, die Kongruenz

(3) $$x_0 + x_1\alpha + x_2\alpha^2 + \cdots + x_{r-1}\alpha^{r-1} \equiv 0 \pmod{\mathfrak{p}}$$

nur dann bestehen, wenn diese Zahlen sämtlich durch p teilbar sind. Da ferner $\mathfrak{p}, \mathfrak{q}$ relative Primideale sind, so kann man immer eine Zahl ϱ so wählen, daß

(4) $$\varrho \equiv 1 \pmod{\mathfrak{p}}, \qquad \varrho \equiv 0 \pmod{\mathfrak{q}},$$

mithin

(5) $$\varrho^2 \equiv \varrho \pmod{p}$$

wird. Setzen wir nun

(6) $$\varrho_0 = \varrho, \ \varrho_1 = \varrho\alpha, \ \varrho_2 = \varrho\alpha^2 \cdots \varrho_{r-1} = \varrho\alpha^{r-1},$$

so sind diese r Zahlen in dem Ideal $\mathfrak{q}$ enthalten, weil ϱ in $\mathfrak{q}$ enthalten ist, und da die Kongruenz

$$x_0\varrho_0 + x_1\varrho_1 + \cdots + x_{r-1}\varrho_{r-1} \equiv 0 \pmod{p}$$

die obige Kongruenz (3) nach sich zieht, so bilden die Zahlen $\varrho_0, \varrho_1 \cdots \varrho_{r-1}$ ein nach p irreduktibles System in $\mathfrak{q}$.

Um für dieses System die Spuren $S(\varrho_\iota \varrho_{\iota'})$ und die zugehörige Determinante R zu bilden, dividieren wir alle Potenzen $1, t, t^2 \cdots$ mit beliebig hohen Exponenten durch $P(t)$, wodurch Gleichungen von der Form

(7) $$t^m = c_0^{(m)} + c_1^{(m)} t + \cdots + c_{r-1}^{(m)} t^{r-1} + P(t) Q_m(t)$$

entstehen, in denen die Koeffizienten $c_\iota^{(m)}$ ganze rationale Zahlen bedeuten; da $Q_m(t)$ ebenfalls eine ganze Funktion mit ganzen rationalen Koeffizienten ist, so folgt

(8) $$\alpha^m \equiv c_0^{(m)} + c_1^{(m)}\alpha + \cdots + c_{r-1}^{(m)}\alpha^{r-1} \pmod{\mathfrak{p}}$$

und hieraus durch Multiplikation mit ϱ

(9) $$\varrho\alpha^m \equiv c_0^{(m)}\varrho_0 + c_1^{(m)}\varrho_1 + \cdots + c_{r-1}^{(m)}\varrho_{r-1} \pmod{p}.$$

Ersetzt man hierin m durch $m+1$, $m+2 \cdots m+r-1$ und bedenkt, daß $\varrho\alpha^m$ eine in $\mathfrak{q}$ enthaltene Zahl μ, und daß $\mu\varrho_\iota = \varrho^2\alpha^{m+\iota} \equiv \varrho\alpha^{m+\iota} \pmod{p}$ ist, so folgt aus dem in 4. bewiesenen Satze

(10) $$S(\varrho\alpha^m) \equiv s_m \pmod{p},$$

www.rcin.org.pl

wo zur Abkürzung

$$s_m = c_0^{(m)} + c_1^{(m+1)} + \cdots + c_{r-1}^{(m+r-1)} \tag{11}$$

gesetzt ist. Da ferner $\varrho_\iota \varrho_{\iota'} = \varrho^2 \alpha^{\iota+\iota'} \equiv \varrho\, \alpha^{\iota+\iota'} \pmod{p}$, und folglich auch

$$S(\varrho_\iota \varrho_{\iota'}) \equiv S(\varrho\, \alpha^{\iota+\iota'}) \equiv s_{\iota+\iota'} \pmod{p} \tag{12}$$

ist, so ergibt sich die entsprechende Determinante

$$R \equiv \begin{vmatrix} s_0, & s_1 \cdots s_{r-1} \\ s_1, & s_2 \cdots s_r \\ s_{r-1}, & s_r \cdots s_{2r-2} \end{vmatrix} \pmod{p}. \tag{13}$$

Um nun zu beweisen, daß diese aus den Zahlen s_m gebildete Determinante E nicht durch p teilbar ist, wollen wir folgenden Weg einschlagen. Bezeichnen wir mit ξ eine Wurzel der irreduktibelen Gleichung r^{ten} Grades

$$P(\xi) = 0, \tag{2'}$$

so ist ξ eine ganze Zahl, und der Inbegriff X aller durch ξ rational darstellbaren Zahlen ist ein Körper r^{ten} Grades, in welchem wir die Normen, Spuren und Diskriminanten resp. durch N', S' und Δ' bezeichnen wollen. Aus den Gleichungen (7) folgt nun zunächst

$$\xi^m = c_0^{(m)} + c_1^{(m)} \xi + \cdots + c_{r-1}^{(m)} \xi^{r-1}, \tag{7'}$$

und da die Zahlen $1, \xi, \xi^2 \cdots \xi^{r-1}$ eine Basis von X bilden, so ist (zufolge § 1, (11))

$$S'(\xi^m) = c_0^{(m)} + c_1^{(m+1)} + \cdots + c_{r-1}^{(m+r-1)} = s_m, \tag{10'}$$

mithin (zufolge § 1, (16)) die Determinante

$$E = \Delta'(1, \xi, \xi^2 \cdots \xi^{r-1})$$

oder (zufolge § 1, (10))

$$E = (-1)^{\frac{r(r-1)}{2}} N'[P'(\xi)]. \tag{14}$$

Da nun $P'(t)$ und $P(t)$ relative Primfunktionen nach dem Modul p sind (§ 3, Anmerkung), so gibt es bekanntlich (K. § 4) zwei Funktionen $\varphi(t)$, $\psi(t)$, welche der Kongruenz

$$\varphi(t) P'(t) + \psi(t) P(t) \equiv 1 \pmod{p}$$

genügen, aus welcher

$$\varphi(\xi) P'(\xi) \equiv 1 \pmod{p}$$

folgt; mithin ist $P'(\xi)$ relative Primzahl zu p; dasselbe gilt folglich (Z. § 174, 2. und 8.) von ihrer Norm, also (zufolge (14)) auch von E und (zufolge (13)) von R, w. z. b. w.

www.rcin.org.pl

Daß die aus den Zahlen s_m gebildete Determinante E nicht durch p teilbar ist, kann man auch ohne Einführung des Körpers X auf folgendem Wege beweisen. Zunächst sind aus den Definitionen (1), (7), (11) die bekannten Formeln abzuleiten:

$$s_{m+r} + a_1 s_{m+r-1} + \cdots + a_r s_m = 0 \tag{15}$$

und, wenn $k < r$,

$$s_k + a_1 s_{k-1} + \cdots + a_k s_0 = (r-k)\, a_k. \tag{16}$$

Drückt man nach (7) die einzelnen Glieder des durch $P(t)$ teilbaren Aggregates

$$P(t)\, t^m = t^{m+r} + a_1 t^{m+r-1} + \cdots + a_r t^m$$

durch die niedrigsten Potenzen von t aus, so ergibt sich

$$c_h^{(m+r)} + a_1 c_h^{(m+r-1)} + \cdots + a_r c_h^{(m)} = 0, \tag{17}$$

wo h jede beliebige der Zahlen $0, 1, 2 \cdots (r-1)$ ist; ersetzt man hierin m durch $(m+h)$ und summiert die so entstandenen Gleichungen für alle Werte von h, so erhält man unter Berücksichtigung von (11) die Gleichung (15). Ist ferner $m < r$, so folgt aus (7), daß

$$c_h^{(m)} = 1 \text{ oder } = 0 \tag{18}$$

ist, je nachdem m und h gleich oder verschieden sind*); ist nun k eine bestimmte der Zahlen $0, 1, 2 \cdots (r-1)$, so folgt aus (18) und (17), daß die Summe

$$c_h^{(k+h)} + a_1 c_h^{(k+h-1)} + \cdots + a_k c_h^{(h)} = a_k \text{ oder } = 0$$

ist, je nachdem

$$h \leqq r-1-k \quad \text{oder} \quad h \geqq r-k$$

ist; durch Summation aller dieser Gleichungen für die verschiedenen Werte von h ergibt sich (16). Hierauf setzen wir

$$P(t) - P(\alpha) = (t-\alpha)(\beta_0 + \beta_1 t + \beta_2 t^2 + \cdots + \beta_{r-1} t^{r-1}),$$

so ist

$$\left\{\begin{array}{ll} \beta_0 & = \alpha^{r-1} + a_1 \alpha^{r-2} + \cdots + a_{r-2}\alpha + a_{r-1} \\ \beta_1 & = \alpha^{r-2} + a_1 \alpha^{r-3} + \cdots + a_{r-2} \\ \cdots & \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \beta_{r-2} & = \alpha + a_1 \\ \beta_{r-1} & = 1 \end{array}\right. \tag{19}$$

*) Hieraus und aus (17) folgt, daß das allgemeine Integral der Differenzengleichung r^{ter} Ordnung

$$y_{m+r} + a_1 y_{m+r-1} + \cdots + a_r y_m = 0$$

durch

$$y_m = c_0^{(m)} y_0 + c_1^{(m)} y_1 + \cdots + c_{r-1}^{(m)} y_{r-1}$$

ausgedrückt wird.

www.rcin.org.pl

und

$$(20)\quad \begin{cases} \alpha\beta_0 &= P(\alpha) - a_r \equiv -a_r\beta_{r-1} \pmod{\mathfrak{p}} \\ \alpha\beta_1 &= \beta_0 - a_{r-1}\beta_{r-1} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ \alpha\beta_{r-2} &= \beta_{r-3} - a_2\beta_{r-1} \\ \alpha\beta_{r-1} &= \beta_{r-2} - a_1\beta_{r-1}. \end{cases}$$

Setzen wir ferner

$$(21)\quad \eta_m = s_m\beta_0 + s_{m+1}\beta_1 + \cdots + s_{m+r-1}\beta_{r-1},$$

so folgt aus (15) und (20)

$$\alpha\eta_m \equiv \eta_{m+1} \pmod{\mathfrak{p}},$$

also

$$\eta_m \equiv \eta_0\alpha^m \pmod{\mathfrak{p}},$$

mithin

$$\eta_0\alpha^m \equiv s_m\beta_0 + s_{m+1}\beta_1 + \cdots + s_{m+r-1}\beta_{r-1} \pmod{\mathfrak{p}}.$$

Wäre nun die aus den Zahlen s_m gebildete Determinante E durch p teilbar, so könnte man nach dem in 1. bewiesenen Satze r ganze rationale Zahlen x_0, $x_1 \cdots x_{r-1}$, die nicht alle durch p teilbar sind, so wählen, daß

$$\left.\begin{array}{llll} s_0 & x_0 + s_1x_1 + \cdots + s_{r-1} & x_{r-1} \equiv 0 \\ s_1 & x_0 + s_2x_1 + \cdots + s_r & x_{r-1} \equiv 0 \\ \cdots\cdots & \cdots\cdots\cdots\cdots & \cdots\cdots \\ s_{r-1}x_0 + s_rx_1 + \cdots + s_{2r-2}x_{r-1} \equiv 0 \end{array}\right\} \pmod{p}$$

wird; dann würde

$$\eta_0(x_0 + x_1\alpha + x_2\alpha^2 + \cdots + x_{r-1}\alpha^{r-1}) \equiv 0 \pmod{\mathfrak{p}},$$

und da der zweite Faktor nicht durch $\mathfrak{p}$ teilbar ist, so wäre

$$\eta_0 = s_0\beta_0 + s_1\beta_1 + \cdots + s_{r-1}\beta_{r-1} \equiv 0 \pmod{\mathfrak{p}};$$

allein es folgt aus (19) und (16), daß

$$\eta_0 = P'(\alpha)$$

und folglich nicht durch $\mathfrak{p}$ teilbar ist; mithin kann auch E, also auch R nicht durch p teilbar sein, w. z. b. w.

§ 6.

Die eben gewonnenen Resultate sind mehr als ausreichend, um auch den zweiten Teil unseres Satzes (§ 3) zu beweisen; derselbe läßt sich in folgender Weise aussprechen:

Geht p in der Grundzahl D des Körpers Ω auf, so ist p in diesem Körper durch das Quadrat eines Primideals teilbar.

www.rcin.org.pl

In der Tat, wenn wir wieder mit $\omega_1, \omega_2 \cdots \omega_n$ eine Basis von $\mathfrak{o}$ bezeichnen, so ist die Grundzahl

$$D = \begin{vmatrix} S(\omega_1\omega_1), & S(\omega_1\omega_2) \cdots S(\omega_1\omega_n) \\ S(\omega_2\omega_1), & S(\omega_2\omega_2) \cdots S(\omega_2\omega_n) \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ S(\omega_n\omega_1), & S(\omega_n\omega_2) \cdots S(\omega_n\omega_n) \end{vmatrix},$$

und wenn dieselbe durch die Primzahl p teilbar ist, so gibt es (zufolge § 5, 1.) n ganze rationale Zahlen $x_1, x_2 \cdots x_n$, welche die Kongruenzen

$$\left.\begin{aligned} x_1 S(\omega_1\omega_1) + x_2 S(\omega_2\omega_1) + \cdots + x_n S(\omega_n\omega_1) &\equiv 0 \\ x_1 S(\omega_1\omega_2) + x_2 S(\omega_2\omega_2) + \cdots + x_n S(\omega_n\omega_2) &\equiv 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ x_1 S(\omega_1\omega_n) + x_2 S(\omega_2\omega_n) + \cdots + x_n S(\omega_n\omega_n) &\equiv 0 \end{aligned}\right\} \pmod{p}$$

befriedigen und nicht alle durch p teilbar sind; setzt man nun

$$\mu = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n,$$

so ist μ nicht teilbar durch p, und die vorstehenden Kongruenzen sind identisch mit den folgenden:

$$S(\mu\omega_1) \equiv 0,\ S(\mu\omega_2) \equiv 0 \cdots S(\mu\omega_n) \equiv 0 \pmod{p};$$

bezeichnet man mit $h_1, h_2 \cdots h_n$ beliebige ganze rationale Zahlen und setzt

$$\omega = h_1\omega_1 + h_2\omega_2 + \cdots + h_n\omega_n,$$

so ist ω eine willkürliche Zahl in $\mathfrak{o}$, und die vorstehenden Kongruenzen lassen sich zusammenfassen in die folgende

$$S(\mu\omega) \equiv 0 \pmod{p};$$

bedeutet ω' ebenfalls eine willkürliche Zahl in $\mathfrak{o}$, so folgt hieraus auch

$$S(\mu\omega + p\omega') \equiv 0 \pmod{p}.$$

Der Inbegriff $\mathfrak{n}$ aller Zahlen ν von der Form $\mu\omega + p\omega'$ ist der größte gemeinschaftliche Teiler der beiden Hauptideale $\mathfrak{o}\mu, \mathfrak{o}p$, also ein Teiler von $\mathfrak{o}p$, und zwar ein echter (d. h. verschieden von $\mathfrak{o}p$), weil μ nicht durch p teilbar ist, und alle in diesem Ideal $\mathfrak{n}$ enthaltenen Zahlen ν genügen der Bedingung

$$S(\nu) \equiv 0 \pmod{p}.$$

Umgekehrt würde sich leicht zeigen lassen, daß hieraus die Teilbarkeit von D durch p folgt.

Nehmen wir nun an, unser Satz sei unrichtig, d. h. $\mathfrak{o}p$ sei ein Primideal oder ein Produkt von lauter verschiedenen Primidealen,

www.rcin.org.pl

so muß es unter denselben wenigstens ein solches $\mathfrak{p}$ geben, welches in dem Ideal $\mathfrak{n}$ nicht aufgeht, weil sonst $\mathfrak{n}$ durch $\mathfrak{o}p$ teilbar wäre. Setzt man dann $\mathfrak{o}p = \mathfrak{p}\mathfrak{q}$, so muß $\mathfrak{q}$ durch $\mathfrak{n}$ teilbar, d. h. jede in $\mathfrak{q}$ enthaltene Zahl λ muß auch in $\mathfrak{n}$ enthalten sein, und folglich sind auch alle Spuren $S(\lambda)$ durch p teilbar. Dies steht aber im Widerspruch mit dem letzten Satze des vorigen Paragraphen; da nämlich nach unserer Annahme $\mathfrak{o}p$ nicht durch $\mathfrak{p}^2$, also $\mathfrak{q}$ nicht durch $\mathfrak{p}$ teilbar ist, so kann man (zufolge § 5, 5.) r Zahlen $\varrho_0, \varrho_1 \cdots \varrho_{r-1}$ aus $\mathfrak{q}$ so auswählen, daß die aus den Spuren $S(\varrho_i \varrho_{i'})$ gebildete Determinante R nicht durch p teilbar ist; da aber die Produkte $\varrho_i \varrho_{i'}$ ebenfalls in $\mathfrak{q}$ enthaltene Zahlen λ sind, deren Spuren folglich durch p teilbar sind, so müßte auch R durch p teilbar sein. Aus diesem Widerspruche folgt, daß unsere Annahme, $\mathfrak{o}p$ sei durch kein Primideal-Quadrat teilbar, unzulässig ist, und hiermit ist unser Satz bewiesen. —

Dieser Satz ist an sich von großem Interesse, und er gestattet zahlreiche wichtige Anwendungen; allein er gibt doch nur ein sehr unvollständiges Bild von der wirklichen Konstitution der Grundzahl D, die wir im folgenden viel genauer erforschen wollen; dabei wird sich von selbst ein neuer, von dem vorstehenden durchaus verschiedener Beweis des genannten Satzes ergeben.

§ 7.

Wir beginnen unsere neue Untersuchung mit einigen Betrachtungen, welche der allgemeinen Theorie der Moduln angehören (Z. § 165). Sind $\mathfrak{a}, \mathfrak{b}$ zwei beliebige Moduln, deren Zahlen wir resp. mit α, β bezeichnen wollen, so besteht ihr größter gemeinschaftlicher Teiler $\mathfrak{d}$ aus allen in der Form $\alpha + \beta$ darstellbaren Zahlen, und ihr kleinstes gemeinschaftliches Vielfaches $\mathfrak{m}$ ist der Inbegriff aller in $\mathfrak{a}$ und $\mathfrak{b}$ gleichzeitig enthaltenen Zahlen $\alpha = \beta$; diese beiden aus $\mathfrak{a}$ und $\mathfrak{b}$ abgeleiteten Moduln $\mathfrak{d}$ und $\mathfrak{m}$ werden wir in der Folge zur Abkürzung resp. mit $\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a}$ und $\mathfrak{a} - \mathfrak{b} = \mathfrak{b} - \mathfrak{a}$ bezeichnen*). Ist η eine bestimmte Zahl, so bedeutet $\mathfrak{a}\eta$ oder $\eta\mathfrak{a}$ den aus allen Produkten $\eta\alpha$ bestehenden Modul, und allgemein wird

*) Von derselben Bezeichnung habe ich in Ermangelung einer besseren auch früher schon Gebrauch gemacht in der Festschrift: Über die Anzahl der Idealklassen in den verschiedenen Ordnungen eines endlichen Körpers (Braunschweig, 1877).

www.rcin.org.pl

unter dem Produkt $\mathfrak{ab}$ der Modul verstanden, dessen Zahlen die Produkte $\alpha\beta$ oder Summen von solchen Produkten sind. Der Quotient

$$\frac{\mathfrak{b}}{\mathfrak{a}} \quad \text{oder} \quad \mathfrak{b}:\mathfrak{a}$$

soll den Inbegriff $\mathfrak{e}$ aller derjenigen Zahlen η bedeuten, für welche $\mathfrak{a}\eta$ durch $\mathfrak{b}$ teilbar wird; sind η', η'' solche Zahlen, so sind alle Produkte $\alpha\eta', \alpha\eta''$ in $\mathfrak{b}$ enthalten, und da $\mathfrak{b}$ ein Modul ist, so sind auch alle Produkte $\alpha(\eta' \pm \eta'')$ in $\mathfrak{b}$ enthalten, d. h. die beiden Moduln $\mathfrak{a}(\eta' \pm \eta'')$ sind ebenfalls teilbar durch $\mathfrak{b}$; mithin gehören die beiden Zahlen $(\eta' \pm \eta'')$ dem System $\mathfrak{e}$ an, welches folglich auch ein Modul ist. Offenbar ist das Produkt $\mathfrak{ae}$ durch $\mathfrak{b}$ teilbar; und wenn $\mathfrak{ac}$ durch $\mathfrak{b}$ teilbar ist, so ist der Modul $\mathfrak{c}$ durch den Quotient $\mathfrak{e}$ teilbar.

Unter der Ordnung $\mathfrak{a}^0$ des Moduls $\mathfrak{a}$ verstehen wir den Quotient

$$\mathfrak{a}^0 = \frac{\mathfrak{a}}{\mathfrak{a}};$$

es leuchtet unmittelbar ein, erstens daß die Zahlen einer solchen Ordnung sich auch durch Multiplikation reproduzieren, und zweitens daß unter ihnen sich auch alle ganzen rationalen Zahlen befinden, daß also der Modul [1] durch $\mathfrak{a}^0$ teilbar ist; aus dieser letzteren Eigenschaft folgt, daß $\mathfrak{a}$ durch $\mathfrak{a}\mathfrak{a}^0$ teilbar ist, und da umgekehrt zufolge der Definition des Quotienten auch $\mathfrak{a}\mathfrak{a}^0$ durch $\mathfrak{a}$ teilbar ist, so ergibt sich der Satz

(1) $$\mathfrak{a}\mathfrak{a}^0 = \mathfrak{a}.$$

Die angeführten beiden Eigenschaften von $\mathfrak{a}^0$ sind charakteristisch für jede Ordnung: ist $\mathfrak{n}$ ein Modul, dessen Zahlen sich auch durch Multiplikation reproduzieren, und ist der Modul [1] teilbar durch $\mathfrak{n}$, so ist $\mathfrak{n}$ gewiß eine Ordnung, nämlich die von $\mathfrak{n}$ selbst, d. h. es ist

(2) $$\mathfrak{n}^0 = \frac{\mathfrak{n}}{\mathfrak{n}} = \mathfrak{n};$$

die erste Eigenschaft besagt nämlich, daß $\mathfrak{n}^2$ durch $\mathfrak{n}$, mithin $\mathfrak{n}$ durch den Quotient $\mathfrak{n}^0$ teilbar ist, und da zufolge der zweiten Eigenschaft $\mathfrak{n}^0$ durch $\mathfrak{n}\mathfrak{n}^0$, also zufolge (1) durch $\mathfrak{n}$ teilbar ist, so ist $\mathfrak{n} = \mathfrak{n}^0$. Zugleich folgt aus (1), wenn $\mathfrak{a} = \mathfrak{n}$ gesetzt wird,

(3) $$\mathfrak{n}^2 = \mathfrak{n}.$$

Diese allgemeinen Betrachtungen wenden wir auf folgenden speziellen Fall an. Es sei Ω wieder ein endlicher Körper n^{ten} Grades,

www.rcin.org.pl

und $\mathfrak{a}, \mathfrak{b}$ seien zwei endliche Moduln, deren Basen zugleich Basen von Ω sind; man überzeugt sich dann leicht, daß die Moduln

$$(4) \qquad \mathfrak{a}+\mathfrak{b},\ \mathfrak{a}-\mathfrak{b},\ \mathfrak{a}\mathfrak{b},\ \frac{\mathfrak{b}}{\mathfrak{a}},\ \mathfrak{a}^0$$

von derselben Beschaffenheit sind. Ist nämlich

$$(5) \qquad \mathfrak{a} = [\alpha_1, \alpha_2 \cdots \alpha_n],\ \mathfrak{b} = [\beta_1, \beta_2 \cdots \beta_n],$$

so folgt

$$\mathfrak{a}+\mathfrak{b} = [\alpha_1, \alpha_2 \cdots \alpha_n, \beta_1, \beta_2 \cdots \beta_n],$$

und nach einem bekannten Satze (Z. § 165, S. 490) kann diese aus $2n$ Zahlen $\alpha_\iota, \beta_\iota$ bestehende Basis auf eine irreduktibele, aus n Zahlen bestehende reduziert werden. Da ferner jede Zahl des Körpers Ω, also auch jede Zahl in $\mathfrak{b}$ durch Multiplikation mit einem von Null verschiedenen rationalen Faktor in eine Zahl des Moduls $\mathfrak{a}$ verwandelt werden kann, so besitzt nach einem anderen Satze (Z. § 165, S. 486) auch $\mathfrak{a}-\mathfrak{b}$ eine aus n Zahlen bestehende, irreduktibele Basis. Für das Produkt und den Quotienten kann man dasselbe in ähnlicher Weise direkt dartun, aber wir ziehen es vor, diese Fälle auf die beiden vorigen durch folgenden Satz zurückzuführen:

Das Produkt $\mathfrak{a}\mathfrak{b}$ ist der größte gemeinschaftliche Teiler der Moduln

$$(6) \qquad \mathfrak{b}\alpha_1, \mathfrak{b}\alpha_2 \cdots \mathfrak{b}\alpha_n,$$

und der Quotient $\mathfrak{b}:\mathfrak{a}$ ist das kleinste gemeinschaftliche Vielfache der Moduln

$$(7) \qquad \mathfrak{b}\alpha_1^{-1}, \mathfrak{b}\alpha_2^{-1} \cdots \mathfrak{b}\alpha_n^{-1}.$$

Hiervon überzeugt man sich leicht; da nämlich jeder der Moduln (6) durch $\mathfrak{a}\mathfrak{b}$ teilbar ist, so gilt dasselbe von ihrem größten gemeinschaftlichen Teiler $\mathfrak{c}$; da ferner jedes Produkt $\alpha\beta$ von der Form $\beta\sum x_\iota\alpha_\iota$, also eine Summe von n Zahlen $(\beta x_\iota)\alpha_\iota$ ist, deren jede einem der n Moduln (6) angehört, so ist $\alpha\beta$ in $\mathfrak{c}$ enthalten, also $\mathfrak{a}\mathfrak{b}$ teilbar durch $\mathfrak{c}$, mithin $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$. Da endlich eine Zahl η stets und nur dann dem Quotienten $\mathfrak{b}:\mathfrak{a}$ angehört, wenn die n Produkte $\eta\alpha_\iota$ in $\mathfrak{b}$, und folglich η in jedem der Moduln (7) enthalten ist, so ist dieser Quotient das kleinste gemeinschaftliche Vielfache der Moduln (7), w. z. b. w.

Nachdem unsere obige Behauptung über die aus $\mathfrak{a}, \mathfrak{b}$ abgeleiteten Moduln (4) hiermit gerechtfertigt ist, wollen wir zur Abkürzung festsetzen, daß unter einem Modul schlechthin und ebenso unter einer Ordnung immer nur ein solcher endlicher Modul verstanden werden soll, dessen Basis zugleich eine Basis des Körpers Ω bildet; nur

www.rcin.org.pl

solche Moduln $\mathfrak{a}, \mathfrak{b} \cdots$ werden im weiteren Verlaufe unserer Untersuchung auftreten. In diesem Sinne gilt zunächst folgender Satz:

Ist $\mathfrak{b}$ teilbar durch $\mathfrak{a}$, so besteht der Quotient $\mathfrak{b} : \mathfrak{a}$ aus lauter ganzen Zahlen, d. h. er ist teilbar durch $\mathfrak{o}$.

Denn wenn η eine beliebige Zahl dieses Quotienten bedeutet, so sind die Produkte $\eta\alpha_1, \eta\alpha_2 \cdots \eta\alpha_n$ in $\mathfrak{b}$, also auch in $\mathfrak{a}$ enthalten, also von der Form $\sum x_\iota \alpha_\iota$, wo $x_1, x_2 \cdots x_n$ ganze rationale Zahlen sind, und hieraus folgt der Satz bekanntlich durch Elimination von $\alpha_1, \alpha_2 \cdots \alpha_n$.

Hieraus folgt von selbst, daß auch jede Ordnung $\mathfrak{a}^0$ oder $\mathfrak{n}$ durch die Ordnung $\mathfrak{o}$ teilbar ist; da ferner die Zahl 1 in $\mathfrak{n}$ enthalten ist, so leuchtet ein, daß

$$\mathfrak{n}\mathfrak{o} = \mathfrak{o} \tag{8}$$

ist. Aus der Teilbarkeit von $\mathfrak{n}$ durch $\mathfrak{o}$ folgt durch abermalige Anwendung desselben Satzes, daß der Quotient

$$\mathfrak{f} = \frac{\mathfrak{n}}{\mathfrak{o}}, \tag{9}$$

welchen wir (wie in § 3 der oben zitierten Festschrift) den Führer der Ordnung $\mathfrak{n}$ nennen wollen, ebenfalls durch $\mathfrak{o}$ teilbar ist. Da die Zahl 1 in $\mathfrak{o}$ enthalten, mithin $\mathfrak{f}$ durch $\mathfrak{f}\mathfrak{o}$ teilbar ist, so folgt aus (9), daß $\mathfrak{f}$ durch $\mathfrak{n}$ teilbar ist; da ferner $\mathfrak{o}^2 = \mathfrak{o}$, also das Produkt $(\mathfrak{f}\mathfrak{o})\mathfrak{o} = \mathfrak{f}\mathfrak{o}$ teilbar durch $\mathfrak{n}$ ist, so muß zufolge (9) auch der erste Faktor $\mathfrak{f}\mathfrak{o}$ durch den Quotienten $\mathfrak{f}$ teilbar sein, mithin ist

$$\mathfrak{f}\mathfrak{o} = \mathfrak{f}, \tag{10}$$

d. h. der Führer $\mathfrak{f}$ ist stets ein Ideal*), und es leuchtet ein, daß jedes durch die Ordnung $\mathfrak{n}$ teilbare Ideal $\mathfrak{a}$ auch durch $\mathfrak{f}$ teilbar ist, weil das Produkt $\mathfrak{o}\mathfrak{a} = \mathfrak{a}$, also durch $\mathfrak{n}$ teilbar ist. Offenbar ist $\mathfrak{o}$ selbst der Führer der Ordnung $\mathfrak{o}$.

§ 8.

Ein anderes wichtiges Hilfsmittel für die genaue Untersuchung der Grundzahl D gewinnen wir durch die folgenden Betrachtungen.

*) Die erforderliche und hinreichende Bedingung, welche ein Ideal $\mathfrak{f}$ erfüllen muß, um Führer einer Ordnung $\mathfrak{n}$ sein zu können, besteht darin, daß, wenn $\mathfrak{p}$ irgend ein in $\mathfrak{f}$ aufgehendes Primideal ersten Grades, und $\mathfrak{f} = \mathfrak{p}\mathfrak{q}$ ist, jede durch das Ideal $\mathfrak{q}$ teilbare rationale Zahl auch durch $\mathfrak{f}$ teilbar ist; unter dieser Voraussetzung bildet das System aller derjenigen Zahlen, welche in bezug auf $\mathfrak{f}$ mit rationalen Zahlen kongruent sind, jedenfalls eine Ordnung $\mathfrak{n}$, deren Führer $\mathfrak{f}$ ist.

www.rcin.org.pl

1. Bilden die ganzen oder gebrochenen Zahlen $\alpha_1, \alpha_2 \cdots \alpha_n$, deren Komplex wir im folgenden kurz durch $((\alpha_\iota))$ bezeichnen wollen, eine Basis des Körpers Ω, so ist bekanntlich ihre Diskriminante A von Null verschieden (Z. § 164, S. 477); da nun (zufolge § 1, (16)) diese Diskriminante

$$A = \begin{vmatrix} S(\alpha_1\alpha_1) \cdots S(\alpha_1\alpha_n) \\ \cdots\cdots\cdots \\ S(\alpha_n\alpha_1) \cdots S(\alpha_n\alpha_n) \end{vmatrix} \tag{1}$$

ist, so gibt es ein und nur ein System $((\alpha'_\iota))$ von n Zahlen $\alpha'_1, \alpha'_2 \cdots \alpha'_n$, welche den n Gleichungen

$$\alpha_r = \sum S(\alpha_r\alpha_\iota)\alpha'_\iota \tag{2}$$

genügen; diese n Zahlen gehören offenbar demselben Körper Ω an und bilden ebenfalls eine Basis von Ω, die wir das Komplement der Basis $((\alpha_\iota))$ nennen wollen. Bei dieser Ausdrucksweise ist wohl darauf zu achten, daß jeder bestimmten Zahl α_r der ersten Basis $((\alpha_\iota))$ eine bestimmte Zahl α'_r der komplementären Basis $((\alpha'_\iota))$ korrespondiert.

2. Ist ω eine beliebige Zahl des Körpers Ω, so sind die n Spuren $S(\omega\alpha_\iota)$ zugleich die Koordinaten von ω in bezug auf die Basis $((\alpha'_\iota))$, d. h. es ist

$$\omega = \sum S(\omega\alpha_\iota)\alpha'_\iota. \tag{3}$$

Da nämlich $((\alpha_\iota))$ eine Basis von Ω ist, so kann ω in die Form $\sum x_\iota\alpha_\iota$ gesetzt werden, wo die Koeffizienten x_ι rationale Zahlen sind, und offenbar folgt aus (2) unmittelbar die allgemeinere Gleichung (3).

3. Bezeichnet man durch das Symbol (r, s) den Wert 1 oder 0, je nachdem die der Reihe $1, 2 \cdots n$ angehörenden Indizes r, s gleich oder ungleich sind, so ist stets

$$S(\alpha_r\alpha'_s) = (r, s). \tag{4}$$

Dies ergibt sich unmittelbar aus (3), wenn man $\omega = \alpha'_s$ setzt.

4. Umgekehrt, wenn zwei Systeme $((\alpha_\iota))$ und $((\beta_\iota))$ den n^2 Relationen

$$S(\alpha_r\beta_s) = (r, s) \tag{5}$$

genügen, so bilden sie zwei Basen des Körpers, von denen jede das Komplement der anderen ist.

Denn zufolge (5) ist die aus den Spuren $S(\alpha_r\beta_s)$ gebildete Determinante $= 1$, also von Null verschieden, woraus (nach § 1, (15)) folgt, daß die Systeme $((\alpha_\iota))$ und $((\beta_\iota))$ Basen des Körpers sind, weil ihre Diskriminanten nicht verschwinden. Mithin besitzt $((\alpha_\iota))$ eine komplementäre Basis $((\alpha'_\iota))$, und da aus (3) und (5)

$$\beta_s = \sum S(\beta_s\alpha_\iota)\alpha'_\iota = \sum (s, \iota)\alpha'_\iota = \alpha'_s$$

www.rcin.org.pl

folgt, so ist $((\alpha_\iota'))$ identisch mit $((\beta_\iota))$. Da ferner die Relationen (5) durchaus symmetrisch in bezug auf beide Systeme sind, so ist ebenso $((\alpha_\iota))$ das Komplement von $((\beta_\iota))$. Es ergibt sich daher auch der Satz:

5. Ist $((\alpha_\iota'))$ das Komplement der Basis $((\alpha_\iota))$, so ist $((\alpha_\iota))$ dasjenige von $((\alpha_\iota'))$. Es gehören daher immer zwei Basen zu einem Paar komplementärer Basen zusammen, und folglich gilt für jede Zahl ω auch die Gleichung

$$\omega = \sum S(\omega \alpha_\iota') \alpha_\iota. \tag{6}$$

6. Wenn zwei Systeme $((\alpha_\iota))$, $((\beta_\iota))$ die Eigenschaft haben, daß für jede Zahl ω die Gleichung

$$\omega = \sum S(\omega \alpha_\iota) \beta_\iota \tag{7}$$

gilt, so bilden sie ein Paar komplementärer Basen.

Denn daraus, daß jede Zahl ω des Körpers in der vorstehenden Form (7) darstellbar ist, folgt zunächst, daß das System $((\beta_\iota))$ eine Basis von Ω ist; und wenn man $\omega = \beta_s$ setzt, so folgen hieraus ferner die Relationen (5).

7. Bezeichnen wir immer mit $((\alpha_\iota'))$ das Komplement der Basis $((\alpha_\iota))$, so ist

$$\sum \alpha_\iota \alpha_\iota' = 1. \tag{8}$$

Denn wenn man ω in (3) durch $\omega \alpha_s'$ ersetzt, so erhält man

$$\omega \alpha_s' = \sum S(\omega \alpha_\iota \alpha_s') \alpha_\iota';$$

hieraus folgt (nach § 1, (11))

$$S(\omega) = \sum S(\omega \alpha_\iota \alpha_\iota') = S\left(\omega \sum \alpha_\iota \alpha_\iota'\right),$$

woraus unser Satz sich ergibt (zufolge § 1, (17) und (18)).

8. Der Koeffizient, welchen das Element $\alpha_m^{(r)}$ in der Determinante

$$\sum \pm \alpha_1^{(1)} \alpha_2^{(2)} \cdots \alpha_n^{(n)} = \sqrt{A} \tag{9}$$

hat, ist

$$= \alpha_m'^{(r)} \sqrt{A}, \tag{10}$$

und folglich ist auch

$$\sum \alpha_\iota^{(r)} \alpha_\iota'^{(s)} = (r, s). \tag{11}$$

In diesem Satze, welcher ohne weiteres aus (4) und bekannten Determinantensätzen folgt, ist der vorige Satz als spezieller Fall enthalten.

9. Ist η von Null verschieden, so sind die Basen $((\eta \alpha_\iota))$ und $((\eta^{-1} \alpha_\iota'))$ komplementär.

www.rcin.org.pl

Dies folgt sofort aus den obigen Sätzen 3. und 4., oder auch aus Gleichung (3), wenn man ω durch $\omega\eta$ ersetzt, durch η dividiert, und den Satz 6. zuzieht.

10. Sind zwei Basen $((\alpha_\iota))$, $((\beta_\iota))$ durch die n Gleichungen

$$\alpha_r = \sum c_{r,\iota}\beta_\iota \tag{12}$$

mit rationalen Koeffizienten $c_{r,s}$ verbunden, so gelten für ihre Komplemente $((\alpha'_\iota))$, $((\beta'_\iota))$ die n Gleichungen

$$\beta'_s = \sum c_{\iota,s}\alpha'_\iota. \tag{13}$$

Denn zufolge (12) und (6) ist $c_{r,s} = S(\alpha_r\beta'_s)$, und hieraus folgt (13) vermöge (3).

11. Die Potenzen $1, \theta, \theta^2 \cdots \theta^{n-1}$ bilden bekanntlich eine Basis des Körpers, wenn die zugehörige Gleichung n^{ten} Grades

$$F(\theta) = 0 \tag{14}$$

irreduktibel ist, d. h. wenn die Zahl

$$\theta^* = F'(\theta) \tag{15}$$

von Null verschieden ist (§ 1); unter dieser Voraussetzung stellen wir uns die Aufgabe, die komplementäre Basis zu finden.

Jede Zahl ω des Körpers läßt sich in der Form $\omega = \psi(\theta)$ darstellen, wo $\psi(t)$ eine ganze Funktion bedeutet, deren Grad $< n$ ist, und deren Koeffizienten rationale Zahlen sind; dann ist bekanntlich

$$\psi(t) = \frac{\psi(\theta^{(1)})}{F'(\theta^{(1)})}\cdot\frac{F(t)}{t-\theta^{(1)}} + \cdots + \frac{\psi(\theta^{(n)})}{F'(\theta^{(n)})}\cdot\frac{F(t)}{t-\theta^{(n)}};$$

setzt man nun die ganze Funktion $(n-1)^{\text{ten}}$ Grades

$$\frac{F(t)}{t-\theta} = \eta_0 + \eta_1 t + \eta_2 t^2 + \cdots + \eta_{n-1}t^{n-1} = \sum \eta_s t^s, \tag{16}$$

so nimmt diese Gleichung folgende Form an:

$$\psi(t) = \sum S\left(\frac{\omega\eta_s}{\theta^*}\right)t^s,$$

und folglich ist

$$\omega = \sum S\left(\frac{\omega\eta_s}{\theta^*}\right)\theta^s.$$

Hieraus ergibt sich nach dem Satze 6., daß die Systeme

$$\left(\left(\frac{\eta_s}{\theta^*}\right)\right) \text{ und } ((\theta^s)) \tag{17}$$

komplementär sind. Setzt man (wie in § 1, (1))

$$F(t) = t^n + a_1 t^{n-1} + \cdots + a_{n-1}t + a_n, \tag{18}$$

www.rcin.org.pl

so ergeben sich für die durch (16) definierten Zahlen η_s folgende Ausdrücke (vgl. § 5, (19)):

$$(19)\quad \begin{cases} \eta_0 = \theta^{n-1} + a_1\theta^{n-2} + \cdots + a_{n-2}\theta + a_{n-1} \\ \eta_1 = \theta^{n-2} + a_1\theta^{n-3} + \cdots + a_{n-2} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \eta_{n-2} = \theta + a_1 \\ \eta_{n-1} = 1. \end{cases}$$

§ 9.

Wir verbinden nun die in den beiden vorhergehenden Paragraphen gewonnenen Resultate miteinander, wobei, wie wir nochmals bemerken, unter einem Modul stets ein solcher endlicher Modul zu verstehen ist, dessen Basis zugleich eine Basis des Körpers Ω bildet.

1. Die beiden Systeme $((\alpha_\iota))$ und $((\beta_\iota))$ bilden bekanntlich stets und nur dann Basen eines und desselben Moduls $\mathfrak{a}$, wenn sie durch n Gleichungen von der Form

$$\alpha_r = \sum c_{r,\iota}\beta_\iota$$

miteinander verbunden sind, wo die Koeffizienten $c_{r,s}$ ganze rationale Zahlen bedeuten, deren Determinante

$$\sum \pm c_{1,1}c_{2,2}\cdots c_{n,n} = \pm 1$$

ist (Z. § 165, S. 489). Da nun (nach § 8, (13)) die zugehörigen komplementären Basen $((\alpha'_\iota))$ und $((\beta'_\iota))$ durch die Gleichungen

$$\beta'_s = \sum c_{\iota,s}\alpha'_\iota$$

miteinander verbunden sind, so bilden sie ebenfalls Basen eines und desselben Moduls, welcher mithin durch den Modul $\mathfrak{a}$ allein schon vollständig bestimmt und von der Wahl der Basis $((\alpha_\iota))$ oder $((\beta_\iota))$ gänzlich unabhängig ist; dieser Modul soll das Komplement von $\mathfrak{a}$ heißen und immer mit $\mathfrak{a}'$ bezeichnet werden. Da ferner (nach § 8, 5.) umgekehrt $((\alpha_\iota))$ die komplementäre Basis von $((\alpha'_\iota))$ ist, so ergibt sich, daß der Modul $\mathfrak{a}$ das Komplement des Moduls $\mathfrak{a}'$ ist, was wir durch die Gleichung

$$(1)\qquad (\mathfrak{a}')' = \mathfrak{a}$$

ausdrücken.

2. Ist $\mathfrak{a}$ teilbar durch $\mathfrak{b}$, so ist $\mathfrak{b}'$ teilbar durch $\mathfrak{a}'$, und zugleich ist $(\mathfrak{b},\mathfrak{a}) = (\mathfrak{a}',\mathfrak{b}')$.

Denn die Basen $((\alpha_\iota))$ und $((\beta_\iota))$ der beiden Moduln $\mathfrak{a}$ und $\mathfrak{b}$ sind durch $2n$ Gleichungen von der Form

$$\alpha_r = \sum c_{r,\iota}\beta_\iota, \quad \beta'_s = \sum c_{\iota,s}\alpha'_\iota$$

www.rcin.org.pl

verbunden, wo die Koeffizienten $c_{r,s}$ ganze rationale Zahlen sind, und der absolute Wert der aus ihnen gebildeten Determinante ist nach einem bekannten Satze (Z. § 165, S. 493) sowohl $= (\mathfrak{b}, \mathfrak{a})$ als $= (\mathfrak{a}', \mathfrak{b}')$.

3. Sind $\mathfrak{a}, \mathfrak{b}$ zwei beliebige Moduln, so ist

$$(2) \qquad (\mathfrak{a} + \mathfrak{b})' = \mathfrak{a}' - \mathfrak{b}'; \quad (\mathfrak{a} - \mathfrak{b})' = \mathfrak{a}' + \mathfrak{b}'.$$

Da nämlich $\mathfrak{a}$ und $\mathfrak{b}$ durch $\mathfrak{a} + \mathfrak{b}$ teilbar sind, so ist (nach 2.) umgekehrt $(\mathfrak{a} + \mathfrak{b})'$ durch $\mathfrak{a}'$ und $\mathfrak{b}'$, also auch durch $\mathfrak{a}' - \mathfrak{b}'$ teilbar. Umgekehrt, da $\mathfrak{a}' - \mathfrak{b}'$ durch $\mathfrak{a}'$ und $\mathfrak{b}'$ teilbar ist, so sind (nach 2.) die Moduln $\mathfrak{a}$ und $\mathfrak{b}$, also auch $\mathfrak{a} + \mathfrak{b}$ durch $(\mathfrak{a}' - \mathfrak{b}')'$ teilbar, woraus wieder (nach 2. und (1)) folgt, daß $\mathfrak{a}' - \mathfrak{b}'$ durch $(\mathfrak{a} + \mathfrak{b})'$ teilbar ist. Aus dieser gegenseitigen Teilbarkeit der beiden Moduln $(\mathfrak{a} + \mathfrak{b})'$ und $\mathfrak{a}' - \mathfrak{b}'$ folgt aber ihre Identität; der zweite Satz (2) ist identisch mit diesem ersten, wie man leicht erkennt, wenn man $\mathfrak{a}, \mathfrak{b}$ resp. durch $\mathfrak{a}', \mathfrak{b}'$ ersetzt und den Satz (1) zuzieht.

4. Sind $\mathfrak{a}, \mathfrak{b}$ zwei beliebige Moduln, so ist

$$(3) \qquad (\mathfrak{b}, \mathfrak{a}) = (\mathfrak{a}', \mathfrak{b}').$$

Denn nach allgemeinen Sätzen (Z. § 165, S. 484) ist

$$(\mathfrak{b}, \mathfrak{a}) = (\mathfrak{a} + \mathfrak{b}, \mathfrak{a}); \quad (\mathfrak{a}', \mathfrak{b}') = (\mathfrak{a}', \mathfrak{a}' - \mathfrak{b}'),$$

und da $\mathfrak{a}$ teilbar durch $\mathfrak{a} + \mathfrak{b}$ ist, so folgt aus den Sätzen 2. und 3., daß

$$(\mathfrak{a} + \mathfrak{b}, \mathfrak{a}) = (\mathfrak{a}', (\mathfrak{a} + \mathfrak{b})') = (\mathfrak{a}', \mathfrak{a}' - \mathfrak{b}')$$

ist, w. z. b. w.

5. Ist η eine von Null verschiedene Zahl des Körpers Ω, so ist

$$(4) \qquad (\mathfrak{a}\,\eta)' = \mathfrak{a}'\,\eta^{-1}.$$

Dies folgt ohne weiteres aus dem Satze 9. in § 8.

6. Mit Zuziehung der komplementären Moduln lassen sich die beiden Operationen der Multiplikation und Division der Moduln aufeinander zurückführen:

$$(5) \qquad (\mathfrak{a}\,\mathfrak{b})' = \frac{\mathfrak{b}'}{\mathfrak{a}} = \frac{\mathfrak{a}'}{\mathfrak{b}}; \qquad \mathfrak{a}\,\mathfrak{b} = \left(\frac{\mathfrak{b}'}{\mathfrak{a}}\right)' = \left(\frac{\mathfrak{a}'}{\mathfrak{b}}\right)'.$$

Da nämlich, wenn $((\alpha_\iota))$ eine Basis von $\mathfrak{a}$ bedeutet, das Produkt $\mathfrak{a}\,\mathfrak{b}$ (zufolge § 7, (6)) der größte gemeinschaftliche Teiler der Moduln

$$\mathfrak{b}\,\alpha_1, \quad \mathfrak{b}\,\alpha_2 \cdots \mathfrak{b}\,\alpha_n$$

ist, so folgt (aus 3.), daß das Komplement $(\mathfrak{a}\,\mathfrak{b})'$ das kleinste gemeinschaftliche Vielfache der Komplemente

$$(\mathfrak{b}\,\alpha_1)', \quad (\mathfrak{b}\,\alpha_2)' \cdots (\mathfrak{b}\,\alpha_n)'$$

ist; da diese letzteren (zufolge 5.) mit

$$\mathfrak{b}'\,\alpha_1^{-1}, \quad \mathfrak{b}'\,\alpha_2^{-1} \cdots \mathfrak{b}'\,\alpha_n^{-1}$$

www.rcin.org.pl

identisch sind, so folgt (nach § 7, (7)), daß $(\mathfrak{a}\mathfrak{b})'$ zugleich der Quotient $\mathfrak{b}' : \mathfrak{a}$ ist. Hiermit ist unser Satz vollständig bewiesen; es wird aber dem Leser vielleicht willkommen sein, wenn wir noch den folgenden, auf Rechnung gegründeten Beweis hinzufügen.

Ist $((\beta_\iota))$ eine Basis von $\mathfrak{b}$, so bilden die n^2 Produkte $\alpha_r \beta_s$ eine Basis des Produktes $\mathfrak{a}\mathfrak{b}$, welche sich nach allgemeinen Sätzen (Z. § 165) auf eine irreduktibele Basis $((\gamma_\iota))$ zurückführen läßt; es gelten dann n^2 Gleichungen von der Form

$$\alpha_r \beta_s = \sum p_\iota^{r,s} \gamma_\iota \tag{6}$$

und umgekehrt n Gleichungen von der Form

$$\gamma_m = \sum q_m^{\iota,\iota'} \alpha_\iota \beta_{\iota'}, \tag{7}$$

wo alle Koeffizienten $p_m^{r,s}$ und $q_m^{r,s}$ ganze rationale Zahlen sind; substituiert man in (7) für die Produkte $\alpha_\iota \beta_{\iota'}$ ihre Ausdrücke gemäß (6), so folgt aus der Irreduktibilität der Basis $((\gamma_\iota))$, daß die Summe

$$\sum p_h^{\iota,\iota'} q_m^{\iota,\iota'} = (h, m), \tag{8}$$

d. h. $= 1$ oder $= 0$ ist, je nachdem h, m gleich oder ungleich sind. Da nun zwischen den Basen $((\alpha_r \beta_\iota))$ und $((\gamma_\iota))$ der Moduln $\mathfrak{b}\alpha_r$ und $\mathfrak{a}\mathfrak{b}$ diejenigen n linearen Relationen (6) stattfinden, in denen r einen und denselben Wert behauptet, so folgen (nach den Sätzen 9. und 10. in § 8) durch den Übergang zu den Komplementen $\mathfrak{b}'\alpha_r^{-1}$ und $(\mathfrak{a}\mathfrak{b})'$ die Gleichungen*)

$$\alpha_r \gamma'_m = \sum p_m^{r,\iota} \beta'_\iota; \tag{9}$$

mithin ist das Produkt $\mathfrak{a}(\mathfrak{a}\mathfrak{b})'$ teilbar durch $\mathfrak{b}'$, also $(\mathfrak{a}\mathfrak{b})'$ teilbar durch den Quotient $\mathfrak{b}' : \mathfrak{a}$. Umgekehrt, wenn η eine beliebige Zahl dieses Quotienten bedeutet, also $\mathfrak{a}\eta$ durch $\mathfrak{b}'$ teilbar ist, so gelten n Gleichungen von der Form

$$\eta \alpha_r = \sum c^{r,\iota} \beta'_\iota, \tag{10}$$

wo die Koeffizienten $c^{r,s}$ ebenfalls ganze rationale Zahlen sind; setzt man ferner

$$e_m = S(\eta \gamma_m), \quad \text{also} \quad \eta = \sum e_\iota \gamma'_\iota, \tag{11}$$

so folgt mit Rücksicht auf (9) die Gleichung

$$\eta \alpha_r = \sum e_\iota \alpha_r \gamma'_\iota = \sum e_\iota p_\iota^{r,\iota'} \beta'_{\iota'};$$

vergleicht man dies mit (10), so folgt

$$c^{r,s} = \sum e_\iota p_\iota^{r,s};$$

*) Dies ergibt sich noch einfacher durch die Bemerkung, daß $p_m^{r,s} = S(\alpha_r \beta_s \gamma'_m)$ ist.

www.rcin.org.pl

multipliziert man jetzt mit $q_m^{r,s}$ und summiert über alle Werte von r, s, so ergibt sich mit Rücksicht auf (8)

$$e_m = \sum c^{\iota,\iota'} q_m^{\iota,\iota'};$$

mithin sind die Zahlen e_m ebenfalls ganze Zahlen, woraus nach (11) folgt, daß η in $(\mathfrak{a}\mathfrak{b})'$ enthalten ist. Also ist der Quotient $\mathfrak{b}' : \mathfrak{a}$ teilbar durch $(\mathfrak{a}\mathfrak{b})'$, und aus dieser gegenseitigen Teilbarkeit beider Moduln folgt ihre Identität, w. z. b. w.

7. Je zwei komplementäre Moduln $\mathfrak{a}, \mathfrak{a}'$ haben dieselbe Ordnung.

Denn setzt man in dem vorigen Satze $\mathfrak{b} = \mathfrak{a}'$, also $\mathfrak{b}' = \mathfrak{a}$, so folgt

$$(\mathfrak{a}\mathfrak{a}')' = \mathfrak{a}^0 = (\mathfrak{a}')^0. \tag{12}$$

8. Ist θ eine ganze Zahl, und zwar Wurzel einer irreduktibelen Gleichung n^{ten} Grades $F(\theta) = 0$, also $\theta^* = F'(\theta)$ von Null verschieden, so ist der Modul

$$\mathfrak{n} = [1, \theta, \theta^2 \cdots \theta^{n-1}] \tag{13}$$

offenbar eine Ordnung, und solche Ordnungen wollen wir reguläre Ordnungen nennen. Durch den Übergang zum Komplement erhält man

$$\theta^* \mathfrak{n}' = [\eta_0, \eta_1 \cdots \eta_{n-1}],$$

wo die Zahlen $\eta_0, \eta_1 \cdots \eta_{n-1}$ durch die Gleichungen (19) in § 8 definiert sind; da nun in unserem Falle, wo θ eine ganze Zahl ist, die Koeffizienten $1, a_1, a_2 \cdots a_n$ der Funktion $F(t)$ ganze rationale Zahlen sind, so bilden offenbar die Zahlen $\eta_0, \eta_1 \cdots \eta_{n-1}$ ebenfalls eine Basis von $\mathfrak{n}$, und folglich ist

$$\theta^* \mathfrak{n}' = \mathfrak{n}. \tag{14}$$

Hieraus folgt durch Multiplikation mit $\mathfrak{o}$ nach dem Satze (8) in § 7

$$\theta^* \mathfrak{o}\mathfrak{n}' = \mathfrak{o},$$

und hieraus (nach dem obigen Satze 5.)

$$(\mathfrak{o}\mathfrak{n}')' = \theta^* \mathfrak{o}'.$$

Bezeichnen wir nun wieder mit $\mathfrak{f}$ den Führer der Ordnung $\mathfrak{n}$ (§ 7, (9)), so ist (nach dem obigen Satze 6.)

$$\mathfrak{f} = \frac{\mathfrak{n}}{\mathfrak{o}} = (\mathfrak{o}'\mathfrak{n}')',$$

mithin

$$\mathfrak{f} = \theta^* \mathfrak{o}'. \tag{15}$$

Bedeutet ferner k wieder den Index der Zahl θ (§ 2), so ist nach (14), (15) und früheren Sätzen

$$k = (\mathfrak{o}, \mathfrak{n}) = (\mathfrak{n}', \mathfrak{o}') = (\theta^* \mathfrak{n}', \theta^* \mathfrak{o}') = (\mathfrak{n}, \mathfrak{f}),$$

www.rcin.org.pl

und da $\mathfrak{k}$ durch $\mathfrak{n}$, ferner $\mathfrak{n}$ durch $\mathfrak{o}$ teilbar ist, so folgt

$$(\mathfrak{o}, \mathfrak{k}) = (\mathfrak{o}, \mathfrak{n})(\mathfrak{n}, \mathfrak{k}),$$

mithin

$$N(\mathfrak{k}) = k^2. \tag{16}$$

Da endlich jede Zahl in $\mathfrak{o}$ durch Multiplikation mit k in eine Zahl der Ordnung $\mathfrak{n}$ verwandelt wird (Z. § 165, S. 485), so ist das Hauptideal $\mathfrak{o}k$ durch $\mathfrak{n}$, folglich auch durch den Führer $\mathfrak{k}$ teilbar (§ 7); mithin gibt es ein und nur ein Ideal $\mathfrak{k}_1$, welches der Bedingung

$$\mathfrak{o}\mathfrak{k} = \mathfrak{k}\mathfrak{k}_1 \tag{17}$$

genügt, und hieraus folgt

$$N(\mathfrak{k}_1) = k^{n-2}. \tag{18}$$

§ 10.

Bezeichnen wir mit $((\omega_\iota))$ eine Basis von $\mathfrak{o}$, mit $((\omega'_\iota))$ die entsprechende Basis des Komplements $\mathfrak{o}'$, so gelten die n Gleichungen

$$\omega_r = \sum S(\omega_r \omega_\iota)\, \omega'_\iota, \tag{1}$$

und da die Spuren der ganzen Zahlen $\omega_r \omega_s$ auch ganze Zahlen sind, so ist $\mathfrak{o}$ teilbar durch $\mathfrak{o}'$; da ferner die Grundzahl

$$D = \begin{vmatrix} S(\omega_1\omega_1) \cdots S(\omega_1\omega_n) \\ \cdots\cdots\cdots\cdots \\ S(\omega_n\omega_1) \cdots S(\omega_n\omega_n) \end{vmatrix} \tag{2}$$

ist, so folgt (Z. § 165, S. 493), daß ihr absoluter Wert

$$(D) = (\mathfrak{o}', \mathfrak{o}) \tag{3}$$

ist, und zugleich leuchtet ein, daß der Modul $D\mathfrak{o}'$ teilbar durch $\mathfrak{o}$ ist. Das Komplement $\mathfrak{o}'$ hat (nach § 9, 7.) dieselbe Ordnung $\mathfrak{o}$, wie $\mathfrak{o}$ selbst; mithin ist $\mathfrak{o}\mathfrak{o}' = \mathfrak{o}'$, also auch $\mathfrak{o}(D\mathfrak{o}') = D\mathfrak{o}'$, und folglich ist der Modul $D\mathfrak{o}'$ ein Ideal. Da ferner, wie schon oben bemerkt, $\mathfrak{o}$ durch $\mathfrak{o}'$ teilbar ist, so ist das Hauptideal $D\mathfrak{o}$ auch teilbar durch das Ideal $D\mathfrak{o}'$, und folglich gibt es ein und nur ein Ideal $\mathfrak{d}$, welches der Bedingung

$$D\mathfrak{o} = \mathfrak{d}(D\mathfrak{o}'), \qquad \mathfrak{o} = \mathfrak{d}\mathfrak{o}' \tag{4}$$

genügt; dieses Ideal $\mathfrak{d}$ wollen wir das Grundideal des Körpers Ω nennen. Aus (3) und einem bekannten Satze der Idealtheorie (Z. § 173, 7.) folgt nun

$$(D) = (D\mathfrak{o}', D\mathfrak{o}) = (D\mathfrak{o}', \mathfrak{d}D\mathfrak{o}') = (\mathfrak{o}, \mathfrak{d}),$$

also erhalten wir den Fundamentalsatz:

$$N(\mathfrak{d}) = (D) \tag{5}$$

www.rcin.org.pl

die Grundzahl eines Körpers ist, absolut genommen, immer die Norm seines Grundideals.

Betrachten wir nun die aus den konjugierten Zahlen $\omega_r^{(s)}$ gebildete Determinante

$$\sum \pm \omega_1^{(1)} \omega_2^{(2)} \cdots \omega_n^{(n)} = \sqrt{D}, \tag{6}$$

so ist $\omega_r' \sqrt{D}$ (nach § 8, 8.) der Koeffizient des Elements ω_r, mithin eine ganze Zahl, weil alle diese Koeffizienten durch Addition, Subtraktion und Multiplikation aus den Elementen $\omega_r^{(s)}$ gebildet werden, welche in unserem Falle ganze algebraische Zahlen sind. Hieraus folgt weiter, daß alle Produkte $D\omega_r'\omega_s'$ aus zwei solchen Zahlen $\omega_r' \sqrt{D}$ und $\omega_s' \sqrt{D}$ ebenfalls ganze Zahlen, mithin in $\mathfrak{o}$ enthalten sind; diese Produkte bilden aber eine (reduktibele) Basis des Moduls

$$D\mathfrak{o}'\mathfrak{o}' = \mathfrak{d}_1, \tag{7}$$

welcher mithin teilbar durch $\mathfrak{o}$ ist. Da ferner, wie schon bemerkt, $\mathfrak{o}\mathfrak{o}' = \mathfrak{o}'$ ist, so folgt $\mathfrak{o}\mathfrak{d}_1 = \mathfrak{d}_1$, mithin ist $\mathfrak{d}_1$ ein Ideal. Multipliziert man nun die Gleichung (4) mit $\mathfrak{o}'$, so folgt

$$D\mathfrak{o}' = \mathfrak{d}\mathfrak{d}_1, \tag{8}$$

also auch

$$D\mathfrak{o} = \mathfrak{d}^2\mathfrak{d}_1. \tag{9}$$

Die Grundzahl D ist daher stets teilbar durch das Quadrat des Grundideals $\mathfrak{d}$, und zugleich ist

$$N(\mathfrak{d}_1) = (D)^{n-2}. \tag{10}$$

Nachdem durch den Satz (5) die Bestimmung der Grundzahl eines Körpers auf diejenige seines Grundideals zurückgeführt ist leuchtet ein, wie wichtig es ist, die Konstitution des letzteren, d. h. seine Zusammensetzung aus Primidealen genau zu erforschen. Für diese Untersuchung, welche in den folgenden Paragraphen ausgeführt werden soll, ist die Betrachtung der regulären Ordnungen erforderlich, und hierzu geben auch die am Schlusse des vorhergehenden Paragraphen gewonnenen Resultate die natürlichste Veranlassung. In der Tat, wenn man dieselben Bezeichnungen beibehält und die dortige Gleichung (15) mit $\mathfrak{d}$ multipliziert, so ergibt sich mit Rücksicht auf die obige Gleichung (4) der wichtige Satz:

$$\mathfrak{o}\theta^* = \mathfrak{d}\mathfrak{k}. \tag{11}$$

Nimmt man die Norm, so erhält man von neuem das schon (aus § 2, (4)) bekannte Resultat

$$N(\theta^*) = \pm Dk^2, \tag{12}$$

www.rcin.org.pl

wo k wieder den Index der Zahl θ bedeutet; da ferner $\mathfrak{o}k = \mathfrak{f}\mathfrak{f}_1$ ist, so folgt mit Rücksicht auf (9)

$$\mathfrak{o}N(\theta^*) = \mathfrak{d}^2\mathfrak{d}_1\mathfrak{f}^2\mathfrak{f}_1^2,$$

also zufolge (11)

$$\mathfrak{o}N(\theta^*) = \theta^*\theta^* \cdot \mathfrak{d}_1\mathfrak{f}_1^2, \tag{13}$$

mithin ist $N(\theta^*)$ stets durch das Quadrat von θ^* teilbar, ein Satz, der auch unmittelbar aus der Definition von θ^* leicht abzuleiten ist.

Aber diese letzten Bemerkungen sind nur von sehr untergeordneter Bedeutung im Vergleich mit dem äußerst wichtigen Satze, welcher in der Gleichung (11) enthalten ist. Das Grundideal $\mathfrak{d}$ ist demnach ein fester gemeinschaftlicher Teiler aller Zahlen θ^*, die allen ganzen Zahlen θ entsprechen, während der andere Faktor $\mathfrak{f}$ von θ abhängig, nämlich der Führer der durch θ erzeugten regulären Ordnung $\mathfrak{n}$ ist; wenn zwei Zahlen θ dieselbe Ordnung $\mathfrak{n}$ erzeugen, so werden folglich die ihnen entsprechenden beiden Zahlen θ^* assoziiert, d. h. ihr Quotient wird eine Einheit sein. Wenn $\mathfrak{o}$ selbst eine reguläre Ordnung ist, wie es z. B. bei jedem quadratischen Körper und auch bei jedem Körper geschieht, der aus einer Gleichung von der Form $\theta^m = 1$ entspringt, so reicht der genannte Satz allein schon aus, um die Konstitution des Grundideals $\mathfrak{d}$ und der Grundzahl D zu bestimmen, weil dann $\mathfrak{o}\theta^* = \mathfrak{d}$ wird. Aber diese Fälle bilden doch nur Ausnahmen unter der unendlichen Mannigfaltigkeit der Körper, und es bedarf daher, um zu unserem Ziele zu gelangen, einer genauen Untersuchung der regulären Ordnungen. Während wir in der früheren Abhandlung (G. § 5) nachgewiesen haben, daß es Körper gibt, in welchen die Indizes k aller Zahlen θ durch eine und dieselbe Primzahl p teilbar sind, so werden wir jetzt zeigen, daß die Führer $\mathfrak{f}$ der entsprechenden regulären Ordnungen $\mathfrak{n}$ niemals alle durch ein und dasselbe Primideal $\mathfrak{p}$ teilbar sind, woraus nach (11) folgt, daß das Grundideal $\mathfrak{d}$ der größte gemeinschaftliche Teiler aller Hauptideale von der Form $\mathfrak{o}\theta^*$ ist.

§ 11.

Um diesen Nachweis zu liefern, benutzen wir die Theorie der höheren Kongruenzen, und um keine Lücken zu lassen, schicken wir, auf die Gefahr hin Bekanntes zu wiederholen, einige Bemerkungen über den Zusammenhang zwischen Zahlenkongruenzen und Funktionenkongruenzen voraus, bei denen es sich immer nur um ganze Funktionen

www.rcin.org.pl

einer Variablen t handelt, deren Koeffizienten ganze rationale Zahlen sind.

Es sei $\mathfrak{p}$ ein bestimmtes Primideal im Körper Ω, und p die durch $\mathfrak{p}$ teilbare positive rationale Primzahl. Wenn nun θ irgend eine ganze Zahl des Körpers, und $F(t)$ wieder die zugehörige Funktion n^{ten} Grades bedeutet (§ 1), so kann man die letztere in bezug auf den Modul p in Primfunktionen $P(t)$ zerlegen, deren höchste Koeffizienten wir immer $= 1$ annehmen (K. § 6); aus dieser Zerlegung

$$F(t) \equiv \Pi P(t) \pmod{p} \tag{1}$$

folgt, weil $F(\theta) = 0$ ist, die Zahlenkongruenz

$$\Pi P(\theta) \equiv 0 \pmod{p}, \tag{2}$$

mithin muß einer der Faktoren, den wir mit $P(\theta)$ bezeichnen wollen, durch das in p aufgehende Primideal $\mathfrak{p}$ teilbar sein, also

$$P(\theta) \equiv 0 \pmod{\mathfrak{p}}. \tag{3}$$

Da eine beliebige Funktion $\psi(t)$ entweder durch $P(t)$ teilbar oder relative Primfunktion zu $P(t)$ ist (mod. p), und da im letzteren Falle eine Kongruenz von der Form

$$\psi(t)\,\psi_1(t) + P(t)\,\psi_2(t) \equiv 1 \pmod{p} \tag{4}$$

stattfindet (K. § 4), so leuchtet ein, daß die Zahlenkongruenz

$$\psi(\theta) \equiv 0 \pmod{\mathfrak{p}} \tag{5}$$

durchaus gleichbedeutend mit der Funktionenkongruenz

$$\psi(t) \equiv 0 \pmod{p,\ P(t)} \tag{5'}$$

ist (K. § 7). Hieraus folgt einerseits, daß die Primfunktion $P(t)$, deren Grad wir mit f bezeichnen wollen, durch die Zahl θ, für welche die Kongruenz (3) gelten soll, vollständig bestimmt ist (mod. p); man würde auch — was aber hier kein weiteres Interesse hat — leicht finden, daß allen und nur denjenigen Zahlen, welche mit einer der f inkongruenten Zahlen

$$\theta,\ \theta^p,\ \theta^{p^2} \dots \theta^{p^{f-1}}$$

nach $\mathfrak{p}$ kongruent sind, dieselbe Primfunktion $P(t)$ entspricht, und daß f ein Divisor vom Grade des Primideals $\mathfrak{p}$ ist. Andererseits ergibt sich aus der Äquivalenz von (5) und (5'), daß zwei ganze Zahlen von der Form $\psi_1(\theta)$, $\psi_2(\theta)$ stets und nur dann nach $\mathfrak{p}$ kongruent sind, wenn die Funktionen $\psi_1(t)$, $\psi_2(t)$ nach dem Doppelmodul p, $P(t)$ kongruent sind, und da p^f die genaue Anzahl aller nach diesem Doppelmodul inkongruenten Funktionen $\psi(t)$ ist (K. § 8), so

www.rcin.org.pl

ist p^f zugleich die Anzahl aller nach $\mathfrak{p}$ inkongruenten Zahlen von der Form $\psi(\theta)$.

Ist daher die Zahl θ die Wurzel einer irreduktibelen Gleichung n^{ten} Grades $F(\theta) = 0$, ist also die entsprechende Zahl $\theta^* = F'(\theta)$ von Null verschieden, so wird, wenn wir wieder die durch θ erzeugte reguläre Ordnung

$$[1,\ \theta,\ \theta^2 \cdots \theta^{n-1}] = \mathfrak{n} \tag{6}$$

setzen,

$$(\mathfrak{n},\ \mathfrak{p}) = p^f. \tag{7}$$

Unter dieser Voraussetzung gilt nun, wenn wir zur Abkürzung

$$P(\theta) = \varrho \tag{8}$$

setzen und mit $\mathfrak{k}$ den Führer der Ordnung $\mathfrak{n}$ bezeichnen, der folgende wichtige Satz:

Die erforderlichen und hinreichenden Bedingungen dafür, daß $\mathfrak{k}$ nicht durch $\mathfrak{p}$ teilbar ist, bestehen darin, erstens, daß f auch der Grad von $\mathfrak{p}$, also

$$N(\mathfrak{p}) = p^f, \tag{9}$$

und zweitens, daß $\mathfrak{p}$ der größte gemeinschaftliche Teiler von $\mathfrak{o}p$ und $\mathfrak{o}\varrho$ ist.

In der Tat, wenn $\mathfrak{k}$ nicht durch $\mathfrak{p}$ teilbar ist, so ist $\mathfrak{o}$ der größte gemeinschaftliche Teiler dieser beiden Ideale und folglich auch derjenige von $\mathfrak{n}$ und $\mathfrak{p}$, weil $\mathfrak{k}$ durch $\mathfrak{n}$, und $\mathfrak{n}$ durch $\mathfrak{o}$ teilbar ist; hieraus folgt nach einem schon oft benutzten Satze (Z. § 165, S. 484)

$$(\mathfrak{n}, \mathfrak{p}) = (\mathfrak{o}, \mathfrak{p}) = N(\mathfrak{p}),$$

woraus sich mit Rücksicht auf (7) die zu beweisende Gleichung (9) ergibt. Ferner leuchtet ein, daß der größte gemeinschaftliche Teiler $\mathfrak{e}$ der Ideale $\mathfrak{o}p, \mathfrak{o}\varrho$ jedenfalls teilbar durch $\mathfrak{p}$ ist, weil zufolge (3) und (8) auch ϱ durch $\mathfrak{p}$ teilbar ist; daß aber wirklich $\mathfrak{e} = \mathfrak{p}$ ist, ergibt sich auf folgende Weise. Da $\mathfrak{k}\mathfrak{p}$ nicht durch $\mathfrak{p}^2$ teilbar ist, so gibt es in $\mathfrak{k}\mathfrak{p}$ eine durch $\mathfrak{p}^2$ nicht teilbare Zahl, welche gewiß von der Form $\psi(\theta)$ ist, weil $\mathfrak{k}\mathfrak{p}$ durch $\mathfrak{k}$, also auch durch $\mathfrak{n}$ teilbar ist; da nun $\psi(\theta)$ durch $\mathfrak{k}\mathfrak{p}$, mithin auch durch $\mathfrak{p}$ teilbar ist, so ist zufolge (5′)

$$\psi(t) \equiv P(t)\,\psi_1(t) \pmod{p},$$

also

$$\psi(\theta) \equiv \varrho\,\psi_1(\theta) \pmod{p},$$

www.rcin.org.pl

woraus sich ergibt, daß die Zahlen p, ϱ nicht beide durch $\mathfrak{p}^2$ teilbar sein können, weil $\psi(\theta)$ nicht durch $\mathfrak{p}^2$ teilbar ist; mithin kann auch $\mathfrak{e}$ nicht durch $\mathfrak{p}^2$ teilbar sein. Ist ferner $\mathfrak{q}$ irgend ein von $\mathfrak{p}$ verschiedenes, in p aufgehendes Primideal, so gibt es in dem Ideal $\mathfrak{f}\mathfrak{q}$, weil es nicht durch $\mathfrak{p}$ teilbar ist, eine durch $\mathfrak{p}$ nicht teilbare Zahl, welche wieder von der Form $\psi(\theta)$ ist, weil $\mathfrak{f}\mathfrak{q}$ durch $\mathfrak{f}$, also auch durch $\mathfrak{n}$ teilbar ist; da $\psi(\theta)$ nicht durch $\mathfrak{p}$, also $\psi(t)$ nicht durch $P(t)$ teilbar ist (mod. p), so gilt die Kongruenz (4), aus welcher, weil p und die in $\mathfrak{f}\mathfrak{q}$ enthaltene Zahl $\psi(\theta)$ durch $\mathfrak{q}$ teilbar sind, die Kongruenz

$$\varrho\,\psi_2(\theta) \equiv 1 \pmod{\mathfrak{q}}$$

folgt; mithin kann ϱ nicht durch $\mathfrak{q}$, also $\mathfrak{e}$ nicht durch $\mathfrak{p}\mathfrak{q}$ teilbar sein. Hieraus folgt offenbar, daß das in p aufgehende Ideal $\mathfrak{e} = \mathfrak{p}$ ist, womit der erste Teil unseres Satzes bewiesen ist.

Wir wenden uns jetzt zu dem bei weitem schwierigeren zweiten Teile: Wenn erstens der Grad f der Primfunktion $P(t)$ zugleich der Grad des Primideals $\mathfrak{p}$, und wenn zweitens $\mathfrak{p}$ der größte gemeinschaftliche Teiler von $\mathfrak{o}p$ und $\mathfrak{o}\varrho$ ist, so haben wir zu zeigen, daß $\mathfrak{f}$ nicht durch $\mathfrak{p}$ teilbar ist. Wir bezeichnen mit $\mathfrak{p}^e$ die höchste in p aufgehende Potenz von $\mathfrak{p}$ und setzen

$$\mathfrak{o}p = \mathfrak{a}\mathfrak{p}^e, \tag{10}$$

wo $\mathfrak{a}$ ein durch $\mathfrak{p}$ nicht teilbares Ideal bedeutet, und wir wollen auf Grund unserer zweiten Annahme zunächst beweisen, daß die Zahlenkongruenz

$$\psi(\theta) \equiv 0 \pmod{\mathfrak{p}^e} \tag{11}$$

mit der Funktionenkongruenz

$$\psi(t) \equiv 0 \pmod{p,\ P(t)^e} \tag{11'}$$

durchaus gleichbedeutend ist; in der Tat leuchtet unmittelbar ein, daß (11) eine Folge von (11') ist; findet aber (11') nicht statt, so ist der größte gemeinschaftliche Teiler, welchen $\psi(t)$ und $P(t)^e$ nach dem Modul p besitzen, von der Form $P(t)^r$, wo $r < e$ ist, und es gilt bekanntlich (K. § 4) eine Kongruenz von der Form

$$\psi(t)\,\psi_1(t) + P(t)^e\,\psi_2(t) \equiv P(t)^r \pmod{p},$$

aus welcher

$$\psi(\theta)\,\psi_1(\theta) \equiv \varrho^r \pmod{\mathfrak{p}^e}$$

folgt; im Falle $e = 1$ (der eigentlich schon oben in (5) und (5') erledigt ist) muß $r = 0$ sein, und folglich kann auch (11) nicht stattfinden; ist aber $e > 1$, also p teilbar durch $\mathfrak{p}^2$, so ist zufolge

www.rcin.org.pl

unserer zweiten Annahme ϱ nicht teilbar durch $\mathfrak{p}^2$, mithin ist $\mathfrak{p}^r$ die höchste in ϱ^r aufgehende Potenz von $\mathfrak{p}$, also ϱ^r nicht teilbar durch $\mathfrak{p}^e$, und folglich kann auch in diesem Falle die Kongruenz (11) nicht stattfinden, was zu zeigen war. Aus dieser Äquivalenz zwischen (11) und (11′) folgt unmittelbar, daß die Anzahl der nach $\mathfrak{p}^e$ inkongruenten Zahlen von der Form $\psi(\theta)$ zugleich die Anzahl der nach dem Doppelmodul $p, P(t)^e$ inkongruenten Funktionen $\psi(t)$ ist, also (K. § 8)

$$(\mathfrak{n}, \mathfrak{p}^e) = p^{ef}.$$

Verbinden wir hiermit unsere erste Annahme (9), so ergibt sich

$$(12) \qquad (\mathfrak{n}, \mathfrak{p}^e) = N(\mathfrak{p}^e) = (\mathfrak{o}, \mathfrak{p}^e),$$

woraus wir schließen, daß $\mathfrak{o}$ der größte gemeinschaftliche Teiler von $\mathfrak{n}$ und $\mathfrak{p}^e$ ist, und daß alle Zahlklassen in bezug auf $\mathfrak{p}^e$ auch durch Zahlen der Ordnung $\mathfrak{n}$ repräsentiert werden können; ist daher ω eine beliebige Zahl in $\mathfrak{o}$, so gibt es immer eine Zahl ν in $\mathfrak{n}$, welche der Bedingung

$$(13) \qquad \omega \equiv \nu \pmod{\mathfrak{p}^e}$$

genügt. Wir ersetzen nun die Kongruenz (1) durch die folgende:

$$(14) \qquad F(t) \equiv A(t) P(t)^m \pmod{p},$$

wo $A(t)$ nach dem Modul p nicht durch $P(t)$ teilbar, also $m \geqq 1$ ist; dann ist zufolge (5) und (5′) die in $\mathfrak{n}$ enthaltene Zahl

$$(15) \qquad \alpha = A(\theta)$$

nicht teilbar durch $\mathfrak{p}$; da ferner $F(\theta) = 0$, mithin

$$(16) \qquad \alpha \varrho^m \equiv 0 \pmod{\mathfrak{a}\mathfrak{p}^e}$$

ist, so folgt

$$(17) \qquad \alpha \equiv 0 \pmod{\mathfrak{a}},$$

weil nach unserer zweiten Annahme ϱ relative Primzahl zu $\mathfrak{a}$ ist. Multipliziert man daher die Kongruenz (13) mit α, so erhält man

$$\omega\alpha \equiv \nu\alpha \pmod{p},$$

also

$$\omega\alpha = \nu\alpha + p\omega_1,$$

wo ω_1 eine ganze Zahl; da aber ν und α, mithin auch $\nu\alpha$ in der Ordnung $\mathfrak{n}$ enthalten ist, so folgt hieraus

$$(18) \qquad \omega\alpha \equiv p\omega_1 \pmod{\mathfrak{n}}.$$

Auf diese Weise kann man aus einer beliebig gewählten ganzen Zahl ω eine Kette von ganzen Zahlen $\omega, \omega_1, \omega_2 \cdots$ bilden, indem man

www.rcin.org.pl

immer $\alpha\omega_r \equiv p\omega_{r+1} \pmod{\mathfrak{n}}$ setzt; da nun jede auf den Modul $\mathfrak{n}$ bezügliche Kongruenz mit jeder in $\mathfrak{n}$ enthaltenen Zahl, also mit p und α multipliziert werden darf, weil $\mathfrak{n}$ eine Ordnung ist, so ergibt sich allgemein, daß

$$\omega\alpha^r \equiv \omega_r p^r \pmod{\mathfrak{n}} \tag{19}$$

ist. Da nun θ die Wurzel einer irreduktibelen Gleichung n^{ten} Grades ist, so kann ihr Index k nicht verschwinden, und folglich kann man

$$k = (\mathfrak{o}, \mathfrak{n}) = hp^s \tag{20}$$

setzen, wo h eine durch p nicht teilbare ganze rationale Zahl bedeutet; setzen wir daher

$$\varkappa = h\alpha^s, \tag{21}$$

so ist $\varkappa$ nicht teilbar durch $\mathfrak{p}$, und da das Hauptideal $\mathfrak{o}k$ durch $\mathfrak{n}$ teilbar ist, so folgt aus (19) und (20)

$$\omega\varkappa \equiv k\omega_s \equiv 0 \pmod{\mathfrak{n}}. \tag{22}$$

Mithin wird jede ganze Zahl ω durch Multiplikation mit $\varkappa$ in eine Zahl der Ordnung $\mathfrak{n}$ verwandelt, d. h. das durch $\mathfrak{p}$ nicht teilbare Ideal $\mathfrak{o}\varkappa$ ist teilbar durch $\mathfrak{n}$; da nun der Führer $\mathfrak{f}$ einer Ordnung $\mathfrak{n}$ in jedem durch $\mathfrak{n}$ teilbaren Ideal aufgeht (§ 7), so ist $\mathfrak{f}$ nicht teilbar durch $\mathfrak{p}$, w. z. b. w.

§ 12.

Nachdem soeben die Bedingungen genau festgestellt sind, unter welchen der Führer einer regulären Ordnung durch ein gegebenes Primideal nicht teilbar ist, wollen wir beweisen, daß diese Bedingungen stets erfüllbar sind, d. h. daß folgender Satz besteht:

Ist $\mathfrak{p}$ ein gegebenes Primideal, so gibt es immer eine reguläre Ordnung $\mathfrak{n}$, deren Führer $\mathfrak{f}$ durch $\mathfrak{p}$ nicht teilbar ist.

In der Tat, wenn p die durch $\mathfrak{p}$ teilbare rationale Primzahl, und f der Grad von $\mathfrak{p}$, also

$$N(\mathfrak{p}) = p^f$$

ist, so wählen wir (wie in § 5, 5. oder in G. § 4) nach Belieben eine Funktion $P(t)$ von demselben Grade f, welche eine Primfunktion in bezug auf den Modul p ist, und unterwerfen die zu suchende Zahl θ, welche die reguläre Ordnung $\mathfrak{n}$ erzeugen soll, zunächst der Bedingung

$$P(\theta) \equiv 0 \pmod{\mathfrak{p}},$$

www.rcin.org.pl

welche Kongruenz bekanntlich immer f Wurzeln besitzt. Für den Fall, daß p durch $\mathfrak{p}^2$ teilbar ist, stellen wir ferner an θ die Forderung, daß $P(\theta)$ nicht durch $\mathfrak{p}^2$ teilbar ist, was sich ebenfalls erreichen läßt, weil die Derivierte $P'(t)$ in bezug auf p relative Primfunktion zu $P(t)$ ist (G. § 4). Ist ferner $\mathfrak{q}$ irgend ein von $\mathfrak{p}$ verschiedenes, in p aufgehendes Primideal, so gibt es jedenfalls Zahlen μ, für welche $P(\mu)$ nicht durch $\mathfrak{q}$ teilbar ist; denn wenn etwa die rationale Zahl $P(0)$ durch $\mathfrak{q}$ und folglich auch durch p teilbar ist, was nur dann geschieht, wenn $P(t) \equiv t \pmod{p}$, so ist $P(1)$ nicht teilbar durch $\mathfrak{q}$, mithin ist mindestens eine der beiden Zahlen 0, 1 eine solche Zahl μ. Wählt man nun die Zahl θ so, daß sie in bezug auf jedes Primideal $\mathfrak{q}$ einer entsprechenden solchen Zahl μ kongruent wird, welche Bedingungen bekanntlich untereinander und auch mit der früheren, auf $\mathfrak{p}$ oder $\mathfrak{p}^2$ bezüglichen verträglich sind, so wird offenbar $\mathfrak{p}$ der größte gemeinschaftliche Teiler von p und $P(\theta)$, und dies bleibt auch bestehen, wenn θ durch irgend eine andere Zahl derselben Zahlklasse (mod. p) ersetzt wird. Die beiden in dem Satze des vorigen Paragraphen aufgestellten charakteristischen Bedingungen sind dann immer erfüllt, und wir haben daher nur noch zu zeigen, daß aus einer solchen Zahlklasse, welche den bisherigen Bedingungen genügt, die Zahl θ immer so ausgewählt werden kann, daß die abgeleitete Zahl θ^* nicht verschwindet, daß also θ die Wurzel einer irreduktibelen Gleichung n^{ten} Grades wird und folglich eine wirkliche Ordnung $\mathfrak{n}$ erzeugt, welche dann unfehlbar die verlangte Eigenschaft besitzen muß. Hierzu gelangt man leicht auf folgende Weise. Da jeder Körper n^{ten} Grades Ω gewiß Zahlen enthält, die einer irreduktibelen Gleichung n^{ten} Grades genügen *), so gibt es unter ihnen auch ganze Zahlen, und es sei ω eine solche; setzen wir wieder fest (wie in § 1), daß die Permutation $\varphi^{(1)}$ alle Zahlen ungeändert läßt, so ist

$$\omega^* = (\omega - \omega^{(2)})(\omega - \omega^{(3)}) \cdots (\omega - \omega^{(n)})$$

und ebenso

$$\theta^* = (\theta - \theta^{(2)})(\theta - \theta^{(3)}) \cdots (\theta - \theta^{(n)}).$$

Ist nun ξ eine bestimmte Zahl, welche allen der Zahl θ oben auferlegten Kongruenzbedingungen genügt, und setzt man

$$\theta = \xi + p\,x\,\omega,$$

*) Dies liegt entweder schon in der Definition von Ω (Z. S. 464, 469), oder es wird leicht bewiesen, falls diese Definition durch eine andere ersetzt wird (zweite Auflage der Zahlentheorie, S. 425, 427).

www.rcin.org.pl

wo x eine willkürliche ganze rationale Zahl bedeutet, so genügt auch diese Zahl θ denselben Bedingungen; da ferner ω^* von Null verschieden ist, so gilt dasselbe von den $(n-1)$ Differenzen $\omega - \omega^{(r)}$, wo r die Werte $2, 3 \cdots n$ durchläuft, und man kann folglich die Zahl x immer so wählen, daß keine der Differenzen

$$\theta - \theta^{(r)} = (\xi - \xi^{(r)}) + p\,x\,(\omega - \omega^{(r)})$$

verschwindet, mithin auch deren Produkt θ^* von Null verschieden wird, w. z. b. w.

Dem Beweise des Satzes wollen wir, um etwaigen Mißverständnissen vorzubeugen, noch folgende Bemerkung hinzufügen. Wenn ein Primideal $\mathfrak{p}$ gegeben ist, so kann man, wie eben bewiesen ist, immer eine reguläre Ordnung konstruieren, deren Führer durch $\mathfrak{p}$ nicht teilbar ist. Sind aber zwei verschiedene Primideale $\mathfrak{p}$, $\mathfrak{q}$ gegeben, so kann schon der Fall eintreten, daß jeder Führer einer regulären Ordnung durch mindestens eins der Ideale $\mathfrak{p}$, $\mathfrak{q}$ teilbar ist. Ein einfaches Beispiel hierfür liefert der in der früheren Abhandlung (G. § 5) betrachtete kubische Körper Ω, dessen Grundzahl $D = -503$ ist*); es ist dort gezeigt, daß der Index k einer jeden ganzen Zahl θ eine gerade Zahl, und daß $\mathfrak{o}(2) = \mathfrak{a}\mathfrak{b}\mathfrak{c}$ ist, wo $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ voneinander verschiedene Primideale ersten Grades bedeuten; und dies reicht hin, um unsere Behauptung mit Zuziehung der jetzigen allgemeinen Theorie zu rechtfertigen. Ist nämlich θ eine bestimmte Zahl und 2^s die höchste in ihrem Index k aufgehende Potenz von 2, so ist $s > 0$, und wenn man mit $\mathfrak{a}^a$, $\mathfrak{b}^b$, $\mathfrak{c}^c$ die höchsten Potenzen von $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ bezeichnet, welche in dem entsprechenden Ordnungsführer $\mathfrak{k}$ aufgehen, so sind die Exponenten a, b, c alle $\leqq s$, weil k immer durch $\mathfrak{k}$ teilbar ist; da ferner $N(\mathfrak{a}) = N(\mathfrak{b}) = N(\mathfrak{c}) = 2$ und $N(\mathfrak{k}) = k^2$ ist (§ 9, (16)), so ist 2^{a+b+c} die höchste in k^2 aufgehende Potenz von 2, folglich $a + b + c = 2s$; mithin kann von den drei Exponenten a, b, c, weil sie $\leqq s$ sind, höchstens einer $= 0$ sein, d. h. $\mathfrak{k}$ ist teilbar durch mindestens zwei der drei Ideale $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ (also auch durch mindestens eins der beiden Ideale $\mathfrak{a}$, $\mathfrak{b}$). Diese theoretischen Vorhersagungen bestätigen sich vollständig durch die wirkliche Rechnung, und man findet z. B. leicht, daß $\mathfrak{a}\mathfrak{c}$, $\mathfrak{b}\mathfrak{c}$, $\mathfrak{a}\mathfrak{b}$ die Führer der regulären Ordnungen sind, welche durch die dort mit α, β, $\alpha + \beta$ bezeichneten Zahlen erzeugt werden.

*) Daß zu dieser Grundzahl nur ein einziger kubischer Körper oder vielmehr drei konjugierte Körper gehören, hängt mit tieferen Gesetzen zusammen, welche den Gegenstand einer anderen Abhandlung bilden sollen.

www.rcin.org.pl

§ 13.

Der im vorigen Paragraphen bewiesene Satz kann mit Rücksicht auf den Satz (11) in § 10 folgendermaßen ausgesprochen werden:

Das Grundideal $\mathfrak{d}$ ist der größte gemeinschaftliche Teiler aller Zahlen $\theta^* = F'(\theta)$, welche allen ganzen Zahlen θ des Körpers entsprechen.

Wir stützen uns nun auf die gewonnenen Resultate, um die Konstitution des Grundideals $\mathfrak{d}$ zu erforschen, d. h. um zu untersuchen, ob und wie oft ein gegebenes Primideal $\mathfrak{p}$ als Faktor von $\mathfrak{d}$ auftritt. Zu diesem Zweck wählen wir die ganze Zahl θ so, daß der Führer $\mathfrak{k}$ der durch sie erzeugten regulären Ordnung $\mathfrak{n}$ nicht durch $\mathfrak{p}$ teilbar ist, und behalten alle in den letzten Paragraphen gebrauchten Bezeichnungen bei. Wir wollen jetzt zeigen, daß die beiden durch die Gleichung (10) und die Kongruenz (14) in § 11 definierten Exponenten e und m einander gleich sind. In der Tat, da die Zahl α nicht durch $\mathfrak{p}$ teilbar ist, so folgt aus der dortigen Kongruenz (16)

$$\varrho^m \equiv 0 \pmod{\mathfrak{p}^e},$$

und hieraus zunächst $m \geqq e$; dies leuchtet unmittelbar ein, wenn $e = 1$ ist; wenn aber $e > 1$, also p durch $\mathfrak{p}^2$ teilbar ist, so kann, wie damals bewiesen ist, ϱ nicht durch $\mathfrak{p}^2$ teilbar sein, mithin ist $\mathfrak{p}^m$ die höchste in ϱ^m aufgehende Potenz von $\mathfrak{p}$, woraus unsere Behauptung folgt. Umgekehrt, da zufolge der dortigen Kongruenz (17) die Zahl α durch das Ideal $\mathfrak{a}$, ferner ϱ durch $\mathfrak{p}$ teilbar ist, so kann man zufolge der dortigen Gleichung (10)

$$\alpha \varrho^e = p\omega$$

setzen, wo ω eine ganze Zahl bedeutet; multipliziert man mit der durch die dortige Gleichung (21) definierten Zahl $\varkappa = h\alpha^s$, so erhält man

$$h\alpha^{s+1}\varrho^e = p\varkappa\omega;$$

nun ist damals in (22) gezeigt, daß $\varkappa\omega$ in $\mathfrak{n}$ enthalten, also eine Zahl von der Form $\psi(\theta)$ ist; die vorstehende Gleichung geht daher, wenn wir noch α und ϱ durch ihre Ausdrücke $A(\theta)$ und $P(\theta)$ ersetzen, in die folgende über:

$$hA(\theta)^{s+1}P(\theta)^e = p\psi(\theta).$$

Hieraus folgt wegen der Irreduktibilität der Gleichung $F(\theta) = 0$ eine Identität von der Form

$$hA(t)^{s+1}P(t)^e = p\psi(t) + F(t)\psi_1(t),$$

www.rcin.org.pl

und da m durch die Kongruenz

$$F(t) \equiv A(t)\,P(t)^m \pmod{p}$$

definiert war, so erhalten wir

$$hA(t)^{s+1}P(t)^e \equiv A(t)\,\psi_1(t)\,P(t)^m \pmod{p}$$

oder auch

$$hA(t)^s P(t)^e \equiv \psi_1(t)\,P(t)^m \pmod{p}.$$

Da nun die rationale Zahl h nicht durch p teilbar, und die Funktion $A(t)$ nicht durch die Primfunktion $P(t)$ teilbar ist (mod. p), so ist $P(t)^e$ die höchste in der linken Seite aufgehende Potenz von $P(t)$, und da die rechte Seite durch $P(t)^m$ teilbar ist, so muß nach dem Fundamentalsatze (K. § 6) in der Theorie der höherer Kongruenzen $e \geqq m$ sein. Oben haben wir aber schon bewiesen, daß $m \geqq e$ ist, und wir erhalten folglich das Resultat

(1) $$m = e,$$

wo e (zufolge § 11, (10)) den Exponenten der höchsten in p aufgehenden Potenz von $\mathfrak{p}$ bedeutet. Zugleich ist also

(2) $$F(t) \equiv A(t)\,P(t)^e \pmod{p},$$

d. h.

$$F(t) = A(t)\,P(t)^e - pM(t),$$

und wir wollen beiläufig bemerken, daß, wenn $e > 1$ ist, die hier auftretende Funktion $M(t)$ nach dem Modul p nicht durch $P(t)$ teilbar sein kann; denn $P(\theta)$ ist in diesem Falle (zufolge § 11) nicht teilbar durch $\mathfrak{p}^2$, und folglich ist $\mathfrak{p}^e$ die höchste Potenz von $\mathfrak{p}$, welche in der linken Seite der Gleichung

$$A(\theta)\,P(\theta)^e = pM(\theta)$$

aufgeht, und da $\mathfrak{p}^e$ auch in p aufgeht, so kann $M(\theta)$ nicht durch $\mathfrak{p}$ teilbar sein, woraus unsere Behauptung folgt, welche von Interesse für die in der früheren Abhandlung (G. § 3) ausgeführte Untersuchung der Funktion $M(t)$ ist.

Durch Differentiation der Kongruenz (2) ergibt sich nun, wenn wir zur Abkürzung

(3) $$B(t) = P(t)\,A'(t) + e\,A(t)\,P'(t)$$

setzen, die folgende Kongruenz:

(4) $$F'(t) \equiv B(t)\,P(t)^{e-1} \pmod{p},$$

aus welcher zunächst

(5) $$\theta^* \equiv B(\theta)\,P(\theta)^{e-1} \pmod{p},$$

also jedenfalls

(6) $$\theta^* \equiv 0 \pmod{\mathfrak{p}^{e-1}}$$

www.rcin.org.pl

folgt. Um aber zu entscheiden, ob $\mathfrak{p}^{e-1}$ die höchste in θ^* aufgehende Potenz von $\mathfrak{p}$ ist, müssen wir zwei wesentlich verschiedene Fälle unterscheiden. Erstens, wenn der Exponent e nicht teilbar durch p ist, so geht aus (3) hervor, daß die Funktion $B(t)$ nach dem Modul p nicht durch $P(t)$ teilbar ist, weil dasselbe auch von $A(t)$ und $P'(t)$ gilt; mithin ergibt sich aus (4), daß $F'(t)$ nach dem Modul p nicht durch $P(t)^e$ teilbar ist, und hieraus folgt nach einem früheren Satze (§ 11, (11) und (11')), daß die Zahl $F'(\theta)$ nicht durch $\mathfrak{p}^e$ teilbar ist; mithin ist in diesem Falle $\mathfrak{p}^{e-1}$ die höchste in der Zahl θ^* aufgehende Potenz von $\mathfrak{p}$. Zweitens, wenn der Exponent e teilbar durch p ist, so ist die Funktion $B(t)$ offenbar durch $P(t)$, mithin $F'(t)$ durch $P(t)^e$ teilbar (mod. p), woraus sich ergibt, daß in diesem Falle die Zahl θ^* mindestens durch $\mathfrak{p}^e$, vielleicht aber auch durch noch höhere Potenzen von $\mathfrak{p}$ teilbar ist.

Da nun der Führer $\mathfrak{k}$ nicht durch $\mathfrak{p}$ teilbar, und (zufolge § 10, (11))

$$\mathfrak{o}\theta^* = \mathfrak{d}\mathfrak{k}$$

ist, so sind die Ideale $\mathfrak{o}\theta^*$ und $\mathfrak{d}$ durch gleich hohe Potenzen von $\mathfrak{p}$ teilbar, und somit erhalten wir den folgenden Fundamentalsatz:

Ist $\mathfrak{p}$ ein beliebiges Primideal, p die durch $\mathfrak{p}$ teilbare rationale Primzahl, und $\mathfrak{p}^e$ die höchste in p aufgehende Potenz von $\mathfrak{p}$, so ist das Grundideal $\mathfrak{d}$ allemal teilbar durch $\mathfrak{p}^{e-1}$; ist ferner der Exponent e nicht teilbar durch p, so ist $\mathfrak{d}$ nicht teilbar durch $\mathfrak{p}^e$; ist aber e teilbar durch p, so ist $\mathfrak{d}$ teilbar durch $\mathfrak{p}^e$ und vielleicht durch noch höhere Potenzen von $\mathfrak{p}$.

§ 14.

Man erkennt leicht, daß der Satz über die Teilbarkeit der Grundzahl D durch eine Primzahl p, von welchem wir in § 3 einen unvollständigen, in den folgenden §§ 4 — 6 aber einen vollständigen Beweis gegeben haben, jetzt aus der Verbindung des eben gewonnenen Resultates über das Grundideal $\mathfrak{d}$ mit dem Satze $N(\mathfrak{d}) = (D)$ unmittelbar hervorgehen muß. In der Tat, wenn die rationale Primzahl p durch das Quadrat eines Primideals $\mathfrak{p}$ teilbar ist, so geht $\mathfrak{p}$ jedenfalls in dem Grundideal $\mathfrak{d}$ auf, dessen Norm (D) mithin durch $N(\mathfrak{p})$, also auch durch p teilbar ist. Umgekehrt, wenn D, also auch $N(\mathfrak{d})$ durch p teilbar ist, so muß nach einem bekannten Satze

www.rcin.org.pl

(Z. § 174, 8.) das Ideal $\mathfrak{d}$ selbst durch ein in p aufgehendes Primideal $\mathfrak{p}$ teilbar sein, und folglich muß $\mathfrak{p}^2$ in p aufgehen, w. z. b. w.

Aber es leuchtet ein, daß wir durch diesen Satz über das Grundideal $\mathfrak{d}$ eine viel tiefere Grundlage gewonnen haben, insofern derselbe die Konstitution dieses Ideals und folglich auch diejenige der Grundzahl D — von gewissen singulären Fällen abgesehen — genau bestimmt. Ein solcher Ausnahmefall tritt nur dann ein, wenn der Exponent e der höchsten in p aufgehenden Potenz von $\mathfrak{p}$ selbst durch p teilbar ist, und da e niemals größer als der Grad n des Körpers sein kann, weil die Norm von $\mathfrak{p}^e$ in p^n aufgeht, so können von der in unserem Satze enthaltenen Unbestimmtheit höchstens solche Primzahlen p getroffen werden, die $\leqq n$ sind. Diese Unbestimmtheit ist auch in der Natur der Sache selbst begründet und nicht etwa einem Mangel in unserer Untersuchung zuzuschreiben; es wird wenigstens nicht leicht sein, diese Ausnahmefälle doch auf bestimmte einfache Gesetze zurückzuführen. In der Tat, wenn der Exponent e durch p teilbar ist, und wenn man mit r den Exponenten der höchsten in $\mathfrak{d}$ aufgehenden Potenz von $\mathfrak{p}$ bezeichnet, so kann es geschehen, daß $r = e$ ist, aber es kann auch $r > e$ sein, ja man kann sogar, wenn irgend ein Vielfaches von e gegeben ist, Fälle nachweisen, in denen r dieses Vielfache überschreitet. Um die große Mannigfaltigkeit der hierbei auftretenden Erscheinungen darzutun, wollen wir nur zwei Beispiele anführen.

Ist Ω ein quadratischer Körper, also $n = 2$, und p eine in der Grundzahl D aufgehende Primzahl, so ist p durch das Quadrat eines Primideals $\mathfrak{p}$ teilbar, und hieraus folgt mit Notwendigkeit, daß

$$\mathfrak{o}p = \mathfrak{p}^2, \quad e = 2, \quad N(\mathfrak{p}) = p, \quad f = 1$$

ist, weil allgemein die Anzahl der Primideale, deren Produkt $= \mathfrak{o}p$ ist, niemals größer als der Grad n des Körpers Ω sein kann. Ist nun p ungerade, also der Exponent e nicht teilbar durch p, so ist das Grundideal $\mathfrak{d}$ durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}^2$ teilbar, und folglich ist dessen Norm (D) durch p, aber nicht durch p^2 teilbar. Ist aber $p = 2$, also der Exponent e teilbar durch p, so ist $\mathfrak{d}$ mindestens durch $\mathfrak{p}^2$, und folglich D mindestens durch 4 teilbar, und es sind zwei Fälle möglich: die höchste in $\mathfrak{d}$ aufgehende Potenz von $\mathfrak{p}$ ist $= \mathfrak{p}^2$ oder $= \mathfrak{p}^3$, je nachdem $\frac{1}{4}D \equiv 3$ oder $\equiv 2 \pmod 4$ ist. In allen Fällen ist

$$\mathfrak{o}D = \mathfrak{d}^2, \quad \mathfrak{o}\sqrt{D} = \mathfrak{d}.$$

www.rcin.org.pl

Wir wollen zweitens den Kreisteilungskörper Ω betrachten, welcher aus einer primitiven Wurzel θ der Gleichung $\theta^m = 1$ entspringt, und dessen Grad $n = \varphi(m)$ ist. Man findet ohne erhebliche Schwierigkeit, daß auch in diesem Falle das Gebiet $\mathfrak{o}$ selbst eine reguläre Ordnung, nämlich

$$\mathfrak{o} = [1, \theta, \theta^2 \cdots \theta^{n-1}],$$

und folglich das Grundideal $\mathfrak{d} = \mathfrak{o}\theta^*$ ist; die Grundzahl D ergibt sich (wenn $m > 2$ ist) aus der Gleichung

$$D \Pi p^{\frac{n}{p-1}} = (-1)^{\frac{1}{2}n} m^n,$$

wo das Produktzeichen Π sich auf alle in m aufgehenden Primzahlen p bezieht. Setzt man ferner

$$m = m' p^s, \quad \varphi(p^s) = e,$$

wo m' nicht teilbar durch p, und bedeutet f den kleinsten positiven Exponenten, für welchen

$$p^f \equiv 1 \pmod{m'}$$

ist, so ist

$$\varphi(m') = af, \quad n = aef,$$

und man findet, daß

$$\mathfrak{o}p = (\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_a)^e$$

ist, wo $\mathfrak{p}_1, \mathfrak{p}_2 \cdots \mathfrak{p}_a$ voneinander verschiedene Primideale vom Grade f sind. Diese Zerlegung gilt für jede Primzahl p, auch wenn sie in m nicht aufgeht und folglich durch kein Primideal-Quadrat teilbar ist ($s = 0$, $e = 1$); uns interessiert aber nur der entgegengesetzte Fall $s > 0$, und dann ist

$$\mathfrak{o}(1 - \theta^{m'}) = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_a.$$

Bezeichnen wir mit $\mathfrak{p}$ irgend eins dieser Primideale, so hat die höchste in p aufgehende Potenz von $\mathfrak{p}$ den Exponenten

$$e = (p-1)\, p^{s-1};$$

bezeichnet man ferner mit r den Exponenten der höchsten in dem Grundideal $\mathfrak{d}$ aufgehenden Potenz von $\mathfrak{p}$, so ist

$$\mathfrak{d} = \mathfrak{a}(1 - \theta^{m'})^r,$$

wo $\mathfrak{a}$ relatives Primideal zu p ist und

$$r = se - \frac{e}{p-1} = (s(p-1) - 1)\, p^{s-1}.$$

Der Exponent e ist nur dann nicht durch p teilbar, und zwar $= p - 1$, wenn $s = 1$, also m nicht teilbar durch p^2 ist, und zugleich ist der

www.rcin.org.pl

Exponent $r = e - 1 = p - 2$; ist aber m teilbar durch p^2, also $s \geqq 2$, so ist e teilbar durch p, und zugleich $r > e$, ausgenommen den Fall $p = 2$, $s = 2$, in welchem $r = e = 2$ ist.

Da man m so wählen kann, daß s beliebig groß ist, so wird hierdurch unsere obige Behauptung gerechtfertigt, daß es Beispiele gibt, in welchen der Exponent r ein beliebiges, gegebenes Vielfaches $(s-1)e$ des Exponenten e überschreitet. Achtet man aber zugleich auf die höchste in e selbst aufgehende Potenz von p (welche in unserem Beispiele $= p^{s-1}$ ist), so scheint es allerdings, als ob sich eine obere Grenze für r angeben lasse, und vielleicht gilt für beliebige Körper der Satz, daß stets $r < se$ ist, wenn $s-1$ der Exponent der höchsten in e aufgehenden Potenz von p ist. Indessen wage ich hierüber keine Vermutung zu äußern, nachdem einige flüchtige Versuche, zu einem Beweise zu gelangen, mir mißglückt sind.

Erläuterungen zur vorstehenden Abhandlung.

In dieser klassisch gewordenen Abhandlung gibt Dedekind zum ersten Male die Grundlage der allgemeinen Verzweigungstheorie in algebraischen Körpern; die große Tragweite der rein arithmetischen Methoden von Dedekind tritt bei der Behandlung dieser Probleme besonders klar hervor.

Die Verzweigungstheorie in der Kroneckerschen Formentheorie (Journ. f. Math., Bd. 92, S. 1—122 (1882)) ist von Hensel (ebenda, Bd. 113, S. 61—83 (1894)) entwickelt worden; unter Anwendung einer etwas anderen Definition der Differente $\mathfrak{d}$ (= Grundideal von Dedekind) erhält man hierin einen einfachen Beweis des ersten Dedekindschen Hauptsatzes

1) $$|D| = N(\mathfrak{d}).$$

In der Henselschen Theorie der p-adischen Zahlen (Hensel, Theorie der algebraischen Zahlen I, Leipzig 1908) werden außer der Kroneckerschen Theorie auch noch arithmetische Methoden angewandt, welche prinzipiell mit den Dedekindschen eine gewisse Ähnlichkeit zeigen.

Weitere Beweise von (1) und dem zweiten Dedekindschen Hauptsatze

$$f'(\theta) = \mathfrak{f} \cdot \mathfrak{d} \qquad (\mathfrak{f} = \text{Führer})$$

findet man bei Hilbert (Jahresber. d. Deutsch. Math. Vereinigung, Bd. 4 (1894)), Landsberg (Gött. Nachr. 1897, S. 277—303), Bauer (Acta litt. ac. scient. reg. univ. Hungaricae, Bd. 1, S. 195—198 (1923), Math. Zeitschr., Bd. 16, S. 1—12 (1923)). Eine besonders einfache Beweisanordnung gibt Hecke (Vorlesungen über die Theorie der algebraischen Zahlen, § 36, Leipzig 1923).

Auf die in der Einleitung versprochenen Behandlung der Verzweigungstheorie in Relativkörpern, ist Dedekind nicht zurückgekommen. Die wichtigsten Resultate auf diesem Gebiete verdankt man Hilbert (l. c. Kap. V). Die eben erwähnte Methode von Hecke läßt sich auch unmittelbar auf Relativkörper verallgemeinern (Hecke, l. c. § 38).

www.rcin.org.pl

Eine Übertragung des Dedekindschen Diskriminantensatzes auf Ringe (Ordnungen) in (endlichen) algebraischen Körpern gab E. Noether (Journ. f. Math., Bd. 157, S. 82—104 (1927)); für die Verzweigungstheorie in Ringen vgl. die in dieser Abhandlung angegebene Literatur.

In der Fußnote am Ende des § 7 gibt Dedekind die notwendige und hinreichende Bedingung dafür, daß ein Ideal Führer eines Ringes (Ordnung) ist. Furtwängler (Sitzungsber. Wien, Abt. IIa, Bd. 128, S. 239—245 (1920)) hat, wahrscheinlich ohne die Dedekindsche Fußnote bemerkt zu haben, ein weiteres Kriterium angegeben, das aber, wie man leicht sieht, mit dem Dedekindschen äquivalent ist (vgl. auch Referat in den Fortschritten d. Math., Bd. 47, S. 146). Die Eigenschaften der Führer der regulären Ringe

$$\mathfrak{n} = [1, \theta, \ldots, \theta^{n-1}]$$

sind von Ore (Math. Ann., Bd. 96, S. 313—352 (1926)) studiert worden.

In seiner Schlußbemerkung spricht Dedekind die Vermutung aus, daß im singulären Falle, wenn die Ordnungszahl e eines Primideals $\mathfrak{p}$ genau durch p^s, $s \geqq 1$ teilbar ist, die Differente genau durch eine Potenz $\mathfrak{p}^\varkappa$ teilbar wird, wo

$$e \leqq \varkappa < (s+1)e \tag{2}$$

gilt. Diese Vermutung wurde zuerst von Hensel (Gött. Nachr. 1897, S. 247—253, Math. Ann., Bd. 55, S. 301—336 (1902)) bewiesen. Weitere Beweise gaben Bauer (Math. Ann., Bd. 83, S. 74—76 (1921)) und Ore (Math. Ann., Bd. 96, S. 313—352 (1926)). Ore (l. c.) hat auch gezeigt, daß zwischen den beiden Grenzen in (2) gewisse Ausnahmewerte vorkommen, welche $\varkappa$ nie annehmen kann, während alle übrigen, nach (2) möglichen Werte von $\varkappa$ auch in passend gewählten Körpern realisiert werden können. (Spezialfälle in den obenerwähnten Arbeiten von Bauer.) Hieraus folgt weiter für ein gegebenes n und p die genaue obere Grenze für die höchste Potenz von p, welche in der Diskriminante eines Körpers n-ten Grades vorkommen kann. Auch hier sind alle möglichen Exponenten bestimmbar. (Spezialfall bei Stickelberger (Intern. Math. Kongreß, Zürich 1897, S. 182—193).) Die Verallgemeinerung der Dedekind-Henselschen Ungleichung (2) auf Relativkörper gab Ore (Math. Ann., Bd. 97, S. 569—598 (1927)).

Für die Körperdiskriminante besteht der bekannte Satz von Minkowski: $|D| > 1$ (Verh. d. Naturf. zu Bremen 1890, Geometrie der Zahlen 1896; weitere Literatur vgl. Dickson, Mitchell, Vandiver, Wahlin, Algebraic numbers § 29. Bulletin of the National Research Council, Vol. 5, no. 28 (1923)).

Ore.

INSTYTUT MATEMAT. P.A.N.

www.rcin.org.pl